L'ANNEXE I REVISE AU DECRET N°2021-916 DU 22 DECEMBRE 2021 PORTANT ADOPTION DU REFERENTIEL GENERAL DE SECURITE DES SYSTEMES D'INFORMATION ET DU PLAN DE PROTECTION DES INFRASTRUCTURES CRITIQUES

Référentiel Général de Sécurité des Systèmes d'Information (RGSSI)

Sommaire

A. *GOUVERNANCE ET CADRE STRATEGIQUE* 6

1. Introduction 6
2. Contexte 6
3. Objectif du référentiel 7
4. Champ d'application 8
5. Contenu du référentiel 8
6. Cadre réglementaire 9

B. DOMAINES D'EXIGENCES 11

D1. Leadership & gouvernance de la sécurité de l'information 11

1.1 Leadership et engagement 11

D2. Politiques de sécurité de l'information 11

2.1 Politiques de sécurité de l'information 11

D3. Organisation de la sécurité de l'information 12

3.1 Fonctions et responsabilités liées à la sécurité de l'information 12

3.2 Séparation des tâches 12

3.3 Contact avec les autorités 12

3.4 Contact avec des groupes d'intérêt spécifiques 13

3.5 Terminaux finaux des utilisateurs 13

3.6 Travail à distance 13

D4. Gestion des risques liés à la sécurité du système d'information 14

4.1 Renseignements sur les menaces 14

4.2 Identification des risques et opportunités 14

4.3 Appréciation des risques de sécurité de l'information 14

4.4 Traitement des risques de sécurité de l'information 15

D5. Sécurité des ressources humaines 15

5.1 Sélection des candidats 15

5.2 Termes et conditions du contrat de travail 15

5.3 Responsabilités de la direction 16

5.4 Sensibilisation, apprentissage et formation à la sécurité de l'information 16

5.5 Processus disciplinaire 17

5.6 Responsabilités après la fin ou le changement d'un emploi 17

D6. Gestion des actifs informationnels 17

6.1 Inventaire des informations et autres actifs associés 17

6.2 Utilisation correcte des informations et autres actifs associés 18

6.3 Restitution des actifs 18
6.4 Classification des informations 18
6.5 Marquage des informations 19
6.6 Gestion des supports de stockage 19
D7. Contrôle d'accès 19
7.1 Contrôle d'accès 19
7.2 Droits d'accès 20
7.3 Gestion des identités 20
7.4 Droit d'accès privilégiés 20
7.5 Informations d'authentification 21
7.6 Restrictions d'accès aux informations 21
7.7 Authentification sécurisée 21
7.8 Utilisation de programmes utilitaires à privilèges 22
7.9 Accès aux codes sources 22
D8. Cryptographie 22
8.1 Utilisation de la cryptographie 22
D9. Sécurité physique et environnementale 23
9.1 Périmètre de sécurité physique 23
9.2 Les entrées physiques 23
9.3 Surveillance de la sécurité physique 23
9.4 Sécurisation des bureaux, des salles et des installations 24
9.5 Protection contre les menaces physiques et environnementales 24
9.6 Travail dans les zones sécurisées 24
9.7 Emplacement et protection du matériel 24
9.8 Services supports 25
9.9 Sécurité du câblage 25
9.10 Maintenance du matériel 25
9.11 Supports de stockage 26
9.12 Sécurité des actifs hors des locaux 26
9.13 Mise au rebut du matériel 26
9.14 Bureau propre et écran vide 27
D10. Sécurité liée à l'exploitation 27
10.1 Procédures d'exploitation documentées 27
10.2 Gestion des configurations 27
10.3 Dimensionnement 28

10.4 Protection contre les programmes malveillants 28
10.5 Filtrage web 28
10.6 Prévention de la fuite de données 28
10.7 Sauvegarde des informations 29
10.8 Suppression sécurisée des informations 29
10.9 Journalisation 29
10.10 Activités de surveillance 30
10.11 Synchronisation des horloges 30
10.12 Installation de logiciels sur des systèmes opérationnels 30
10.13 Gestion des vulnérabilités techniques 30
10.14 Protection des systèmes d'information pendant les tests d'audit 31
D11. Sécurité des communications 31
11.1 Sécurité des réseaux 31
11.2 Sécurité des services réseaux 31
11.3 Cloisonnement des réseaux 32
11.4 Transfert des informations 32
11.5 Accords de confidentialité ou de non-divulgation 32
D12. Acquisition, développement et maintenance des systèmes d'information 33
12.1 Sécurité de l'information dans la gestion de projet 33
12.2 Exigences de sécurité des applications 33
12.3 Cycle de vie de développement sécurisé 33
12.4 Codage sécurisé 34
12.5 Gestion des changements 34
12.6 Principes d'ingénierie et d'architecture des systèmes sécurisés 34
12.7 Séparation des environnements de développement, de test et d'exploitation 34
12.8 Développement externalisé 35
12.9 Informations de test 35
12.10 Masquage des données 35
D13. Relations avec les fournisseurs 36
13.1 La sécurité de l'information dans les accords conclus avec les fournisseurs 36
13.2 Sécurité de l'information dans l'utilisation de services cloud 36
13.3 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC 36
13.4 Surveillance, révision et gestion des changements des services fournisseurs 37
D14. Gestion des incidents de sécurité de l'information 37
14.1 Planification et préparation de la gestion des incidents de sécurité de l'information 37

14.2 Déclaration des événements de sécurité de l'information 38
14.3 Évaluation des événements de sécurité de l'information et prise de décision 38
14.4 Réponse aux incidents de sécurité de l'information 38
14.5 Tirer des enseignements des incidents de sécurité de l'information 39
14.6 Collecte des preuves 39
D15. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 39
15.1 Sécurité de l'information pendant une perturbation 39
15.2 Redondance des moyens de traitement de l'information 40
15.3 Préparation des TIC pour la continuité d'activité 40
D16. Conformité 40
16.1 Exigences légales, statutaires, réglementaires et contractuelles 40
16.2 Droits de propriété intellectuelle 41
16.3 Protection des enregistrements 41
16.4 Protection de la vie privée et des données à caractère personnel 41
16.5 Révision interne de la sécurité de l'information 42
16.6 Conformité aux politiques, règles et normes de sécurité de l'information 42

A. *GOUVERNANCE ET CADRE STRATEGIQUE*

1. Introduction

À l'ère du numérique, les systèmes d'information sont devenus des piliers essentiels du fonctionnement des États, des entreprises et des citoyens. Cependant, leur interconnexion croissante et leur dépendance aux technologies digitales les rendent particulièrement vulnérables aux cybermenaces. Les attaques informatiques, de plus en plus sophistiquées et fréquentes, mettent en péril la sécurité des données, la continuité des services et la confiance des utilisateurs.

Face à cette réalité, la Côte d'Ivoire, comme de nombreux pays, a pris des mesures concrètes pour protéger son cyberespace. La création de l'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** par décret N° 2024-958 du 30 octobre 2024 s'inscrit dans cette dynamique. Cette agence a pour mission de protéger les systèmes d'information nationaux, de sécuriser les infrastructures critiques et de promouvoir une culture de sécurité numérique.

Dans le cadre de ses attributions, l'ANSSI élabore des normes et référentiels destinés à encadrer les pratiques de sécurité des systèmes d'information. Le présent Référentiel s'inscrit dans cette logique, en fournissant un cadre structuré pour accompagner les acteurs publics et privés dans la mise en œuvre des mesures de sécurité conformes aux exigences nationales.

2. Contexte

La Côte d'Ivoire, à l'instar des nations engagées dans une transformation numérique, reconnaît que le développement des technologies numériques s'accompagne d'une recrudescence des risques cybernétiques. Face à cette réalité, l'Etat a pris le décret n° 2021-916 du 22 décembre 2021 portant adoption du **Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) et du Plan de Protection des Infrastructures Critiques (PPIC)**. Ce dit décret dispose en son article 2 : « **Les organismes publics et les entreprises privées sont tenues de se conformer au RGSSI et au PPIC** ». Il met en place un cadre normatif visant à renforcer la sécurité des systèmes d'information des administrations publiques et des entreprises privées.

Cette version 2021 du référentiel s'appuyait sur les normes internationales, ISO/IEC 27001:2013 et ISO/IEC 27002:2013. La multiplication des cyberattaques, les activités illicites dans le cyberespace et la révision des normes ISO ont rendu obsolètes certaines dispositions du **Référentiel Général de Sécurité des Systèmes d'Information (RGSSI)** initial, ne permettant plus de répondre efficacement aux menaces contemporaines. C'est dans ce contexte que s'inscrit la révision du référentiel qui permettra d'intégrer les nouvelles pratiques de cybersécurité, adapter les contrôles aux menaces émergentes et renforcer la souveraineté nationale.

Le présent référentiel définit les principes, règles et exigences transversales applicables à l'ensemble des acteurs publics et privés, sans distinction de secteurs. A l'avenir, ce référentiel général fera l'objet de déclinaisons spécifiques afin de tenir compte des particularités opérationnelles et du niveau d'exposition propre à chaque domaine.

3. Objectif du référentiel

L'objectif de ce référentiel est d'évaluer la maturité et la conformité des systèmes d'information. C'est la norme ivoirienne en matière de sécurité des systèmes d'information. Les principaux objectifs sont :

- Adapter les exigences de sécurité aux nouveaux usages numériques ;
- Intégrer les retours d'expérience issus des audits et des incidents ;
- Favoriser l'adoption par les administrations et les organismes privés de bonnes pratiques en matière de sécurité des systèmes d'information ;
- Adapter les solutions techniques aux justes besoins de sécurité identifiés pour chaque système d'information.

Le schéma général du cadre normatif ci-dessous est composé de :

1. **ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)**
    - Élabore, met en œuvre, évalue et améliore le cadre normatif.
2. **RGSSI (Référentiel Général de Sécurité des Systèmes d'Information)**
    - Référentiel central, conforme aux normes **ISO/IEC 27001 et 27002**.
3. **RA-RGSSI (Référentiel d'Application du RGSSI)**
    - Détaille les recommandations de mise en œuvre de chaque mesure de sécurité évoquée dans le RGSSI.
4. **PASSI (Prestataire d'Audit de Sécurité des Systèmes d'Information)** et **Auditeur en SSI**
    - Acteurs habilités à réaliser les audits selon le référentiel.
5. **Organisme audité**
    - Soumis à des audits réglementaires.
6. **Centre de formation agréée**
    - Responsable de la formation et de l'évaluation des auditeurs selon le RGSSI.
7. **Auditeur en SSI**
    - Réalise les audits de conformité selon le RGSSI.

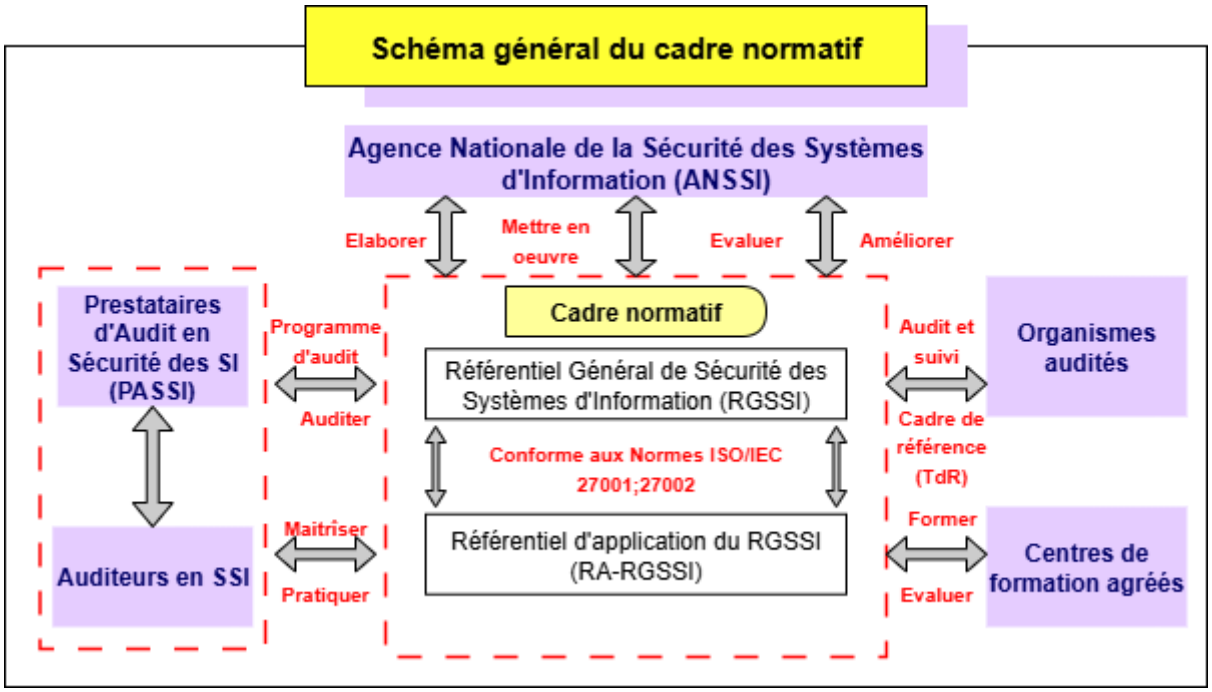

Figure 1. Schéma général du cadre normatif

4. Champ d'application

Ce référentiel est applicable à tous les organismes soumis à l'obligation d'audit conformément aux exigences du décret n° 2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information.

5. Contenu du référentiel

L'audit de la sécurité des systèmes d'information constitue une étape clé dans le renforcement du niveau de maturité en cybersécurité. Il vise à instaurer un juste équilibre entre les risques liés à l'usage des technologies de l'information et les avantages qu'elles procurent. Cette démarche permet d'optimiser de manière mesurable, pertinente et efficiente les processus associés. Le Référentiel Général de Sécurité des Systèmes d'Information s'articule autour de 16 domaines principaux :

D1. Leadership et gouvernance de la sécurité de l'information
D2. Politiques de sécurité de l'information
D3. Organisation de la sécurité de l'information
D4. Gestion des risques liés à la sécurité de l'information
D5. Sécurité des ressources humaines
D6. Gestion des actifs informationnels
D7. Contrôle d'accès
D8. Cryptographie
D9. Sécurité physique et environnementale

D10. Sécurité liée à l'exploitation
D11. Sécurité des communications
D12. Acquisition, développement et maintenance des systèmes d'information
D13. Relations avec les fournisseurs
D14. Gestion des incidents liés à la sécurité de l'information
D15. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
D16. Conformité

Les 16 domaines du RGSSI regroupent un total de 107 critères de vérification, chacun étant associé à un niveau d'exigence déterminé en fonction de la criticité de la donnée traitée par l'organisme audité.

- Niveau 1 : Ce niveau concerne les structures à faible exposition, qui n'exploitent pas essentiellement de données sensibles. Une compromission de leur système n'aura pas d'impact direct sur la sécurité nationale. Ces entités doivent mettre en œuvre des mesures de sécurité minimales pour assurer la confidentialité, la disponibilité et l'intégrité de leurs informations.

- Niveau 2 : Ce niveau concerne les organismes qui traitent des données sensibles ou à caractère personnel. Compte tenu des risques associés, ces structures doivent mettre en place et appliquer des mesures de manière systématique, rigoureuse et régulière afin de garantir la confiance de leurs parties prenantes.

- Niveau 3 : Ce niveau s'applique aux organismes qui exploitent des données d'intérêt vital pour la nation. Toute compromission de leurs activités aurait un impact majeur sur la sécurité nationale, la défense ou l'ordre public. Ces structures sont donc soumises au niveau d'exigence le plus élevé et doivent appliquer les mesures de sécurité avec une rigueur absolue en veillant à anticiper toute menace significative.

6. Cadre réglementaire

La gouvernance de la sécurité des systèmes d'information en Côte d'Ivoire est régie par un ensemble de textes juridiques nationaux et des normes internationales. Ces instruments constituent la base légale et normative qui encadre la sécurisation des transactions électroniques, ainsi que la mise en œuvre des bonnes pratiques de sécurité.

- Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;
- Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Loi n°2024-352 du 06 juin 2024 relative aux communications électroniques ;

- Décret n°2024-958 du 30 octobre 2024 portant création, attributions, organisation et fonctionnement de l'Agence Nationale de la Sécurité des Systèmes d'Information ;
- Décret n°2021-915 du 22 décembre 2021 portant adoption de la politique de sécurité des systèmes d'information de l'administration publique ;
- Décret n°2021-916 du 22 décembre 2021 portant adoption du RGSSI et du PPIC ;
- Décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information ;
- ISO/IEC 27001:2022, système de management de la sécurité de l'information ;
- ISO/IEC 27002:2022, code de bonnes pratiques pour le management de la sécurité de l'information ;
- ISO/IEC 19011:2018, lignes directrices pour l'audit des systèmes de management.

B. DOMAINES D'EXIGENCES

D1. Leadership & gouvernance de la sécurité de l'information

1.1 Leadership et engagement

Mesure de sécurité	N1	N2	N3
La direction doit faire preuve de leadership et affirmer son engagement en faveur de la sécurité de son système d'information.		✓	✓
La direction doit formaliser un Plan Annuel de Sécurisation (PAS) : exigences, actions, moyens, responsabilités et plan d'action.			✓

Objectif

Garantir que la sécurité devienne une priorité stratégique clairement affichée et intégrée à tous les niveaux de l'organisation.

D2. Politiques de sécurité de l'information

2.1 Politiques de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit élaborer, documenter, obtenir l'approbation de la direction, diffuser largement et réviser régulièrement une Politique de Sécurité des Systèmes d'Information (PSSI) et des politiques thématiques. Elle doit s'assurer de la compréhension, de l'adhésion du personnel et des parties intéressées via des mécanismes de validation et de formation continue.		✓	✓

Objectif

Assurer de manière continue la pertinence, l'adéquation, l'efficacité des orientations de la direction et de son soutien à la sécurité de l'information selon les exigences métier, légales, statutaires, réglementaires et contractuelles.

D3. Organisation de la sécurité de l'information

3.1 Fonctions et responsabilités liées à la sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit définir, documenter et attribuer formellement les rôles et responsabilités en matière de sécurité de l'information (y compris la désignation d'un Responsable de la Sécurité des Systèmes d'Information - RSSI), en s'assurant que ces rôles sont dotés des compétences et des ressources nécessaires.		✓	✓

Objectif

Établir une structure définie, approuvée et comprise pour la mise en œuvre, le fonctionnement et la gestion de la sécurité de l'information au sein de l'organisation.

3.2 Séparation des tâches

Mesure de sécurité	N1	N2	N3
L'organisation doit identifier et séparer les tâches critiques et incompatibles (ex : développement et production, gestion des accès et audit) afin de réduire le risque d'actions frauduleuses ou d'erreurs non détectées.		✓	✓

Objectif

Réduire le risque de fraude, d'erreur et de contournement des mesures de sécurité de l'information.

3.3 Contact avec les autorités

Mesure de sécurité	N1	N2	N3
L'organisation doit établir et maintenir le contact avec les autorités appropriées.	✓	✓	✓
L'organisation doit conclure un accord formel de partenariat avec l'ANSSI (CI-CERT).			✓

Objectif

Assurer la circulation adéquate de l'information en matière de sécurité de l'information, entre l'organisation et les autorités légales, réglementaires et de surveillance pertinente.

3.4 Contact avec des groupes d'intérêt spécifiques

Mesure de sécurité	N1	N2	N3
L'organisation doit établir et maintenir des contacts avec des groupes d'intérêt spécifiques ou autres forums spécialisés sur la sécurité et associations professionnelles.		✓	✓
L'organisation doit participer à des groupes de travail et des cadres d'échanges permanents animés par l'ANSSI.			✓

Objectif

Assurer la circulation adéquate de l'information en matière de sécurité de l'information.

3.5 Terminaux finaux des utilisateurs

Mesure de sécurité	N1	N2	N3
L'organisation doit protéger les informations stockées, traitées ou accessibles via des terminaux finaux des utilisateurs.	✓	✓	✓

Objectif

Protéger les informations contre les risques liés à l'utilisation de terminaux finaux des utilisateurs.

3.6 Travail à distance

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre des mesures de sécurité lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées, stockées ou en transit en dehors des locaux de l'organisation.	✓	✓	✓

Objectif

Assurer la sécurité des informations lorsque le personnel travaille à distance.

D4. Gestion des risques liés à la sécurité du système d'information

4.1 Renseignements sur les menaces

Mesure de sécurité	N1	N2	N3
L'organisation doit collecter et analyser les informations relatives aux menaces de sécurité de l'information pour produire les renseignements sur les menaces.		✓	✓

Objectif

Assurer une compréhension globale du contexte interne et externe afin d'identifier les risques et opportunités pertinents, et ainsi garantir une gestion proactive et adaptée de la sécurité du système d'information.

4.2 Identification des risques et opportunités

Mesure de sécurité	N1	N2	N3
L'organisation doit tenir compte des enjeux et des exigences, et déterminer les risques et opportunités qui nécessitent d'être abordés pour sécuriser son système d'information.		✓	✓

Objectif

Anticiper sur les évènements susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs.

4.3 Appréciation des risques de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information.		✓	✓

Objectif

Ce processus permet d'évaluer et de classifier les risques liés à la sécurité de l'information, afin de faciliter le processus de remédiation en fonction de leur criticité et de l'impact sur les actifs de l'organisation.

4.4 Traitement des risques de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit établir et maintenir un processus structuré annuel d'appréciation des risques de sécurité de l'information, incluant l'identification, l'analyse (probabilité et impact) et l'évaluation des risques, en tenant compte des actifs, des menaces et des vulnérabilités, et en alignement avec sa tolérance au risque.		✓	✓
L'organisation doit réaliser une analyse de risques complète sur tout le périmètre critique, à renouveler au moins tous les 6 mois.			✓

Objectif

Fournir une vision priorisée des risques qui orientera les décisions de sécurité en cohérence avec la stratégie de l'entreprise et sa tolérance au risque.

D5. Sécurité des ressources humaines

Avant l'embauche

5.1 Sélection des candidats

Mesure de sécurité	N1	N2	N3
L'organisation doit effectuer des vérifications d'antécédents (références, casier judiciaire, etc.) proportionnées aux responsabilités du poste et à l'accès aux informations sensibles, avant l'embauche du personnel.	✓	✓	✓

Objectif

S'assurer que tous les membres du personnel sont éligibles et adéquats pour remplir les fonctions pour lesquelles ils sont candidats, et qu'ils le restent tout au long de leur emploi.

5.2 Termes et conditions du contrat de travail

Mesure de sécurité	N1	N2	N3
L'organisation doit s'assurer que les contrats de travail indiquent les responsabilités du personnel et de l'organisation en matière de sécurité de l'information.	✓	✓	✓

Objectif

S'assurer que le personnel comprend ses responsabilités en termes de sécurité de l'information dans le cadre des fonctions que l'organisation envisage de lui confier.

Pendant la durée du contrat

5.3 Responsabilités de la direction

Mesure de sécurité	N1	N2	N3
La direction doit demander à tout le personnel d'appliquer les mesures de sécurité de l'information conformément à la politique de sécurité de l'information, aux politiques spécifiques à une thématique et aux procédures établies de l'organisation.		✓	✓

Objectif

S'assurer que la direction comprend son rôle en matière de sécurité de l'information et qu'elle entreprend des actions visant à garantir que tout le personnel est conscient de ses responsabilités liées à la sécurité de l'information et qu'il les mène à bien.

5.4 Sensibilisation, apprentissage et formation à la sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en place un programme continu de sensibilisation, de formation et d'évaluation des connaissances en matière de sécurité de l'information pour l'ensemble du personnel et des parties intéressées, adapté à leurs rôles et responsabilités, et incluant des simulations pour renforcer la vigilance.	✓	✓	✓
L'organisation doit établir un plan de formation annuel spécifique pour le personnel affecté à la gestion opérationnelle des infrastructures critiques.			✓

Objectif

S'assurer que le personnel et les parties intéressées pertinentes connaissent et remplissent leurs responsabilités en matière de sécurité de l'information.

5.5 Processus disciplinaire

Mesure de sécurité	N1	N2	N3
L'organisation doit formaliser et communiquer un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées ayant commis une violation de la politique de sécurité de l'information.		✓	✓

Objectif

S'assurer que le personnel et d'autres parties intéressées comprennent les conséquences des violations de la politique de sécurité de l'information, prévenir ces violations et traiter de manière appropriée ces violations commises.

Rupture terme ou modification du contrat de travail

5.6 Responsabilités après la fin ou le changement d'un emploi

Mesure de sécurité	N1	N2	N3
L'organisation doit maintenir et faire respecter les obligations de confidentialité et de non-divulgation après la fin ou la modification d'un contrat de travail ou de prestation.	✓	✓	✓

Objectif

Protéger les intérêts de l'organisation dans le cadre du processus de changement ou de fin d'un emploi ou d'un contrat.

D6. Gestion des actifs informationnels

6.1 Inventaire des informations et autres actifs associés

Mesure de sécurité	N1	N2	N3
L'organisation doit établir et maintenir un inventaire exhaustif et précis de tous les actifs informationnels et physiques (matériels, logiciels, services, données) supportant les systèmes d'information, en identifiant clairement leur propriétaire, leur classification de sécurité et leur valeur pour l'organisation.	✓	✓	✓

L'organisation doit tenir un inventaire semestriel de ses actifs informationnels qui doit être transmis à l'ANSSI dans des conditions sécurisées.			✓

Objectif

Identifier les informations et autres actifs associés de l'organisation afin de préserver leur sécurité et d'en attribuer la propriété de manière appropriée.

6.2 Utilisation correcte des informations et autres actifs associés

Mesure de sécurité	N1	N2	N3
L'organisation doit identifier, documenter et mettre en œuvre les règles d'utilisation correcte et les procédures de traitement des informations et autres actifs associés.	✓	✓	✓

Objectif

Assurer que les informations et autres actifs associés sont protégés, utilisés et traités de manière appropriée.

6.3 Restitution des actifs

Mesure de sécurité	N1	N2	N3
Le personnel et les autres parties intéressées, selon le cas, doivent restituer tous les actifs de l'organisation qui sont en leur possession au moment du changement ou de la fin de leur emploi, contrat ou accord.	✓	✓	✓

Objectif

Protéger les actifs de l'organisation dans le cadre du processus du changement ou de la fin de leur emploi, contrat ou accord.

6.4 Classification des informations

Mesure de sécurité	N1	N2	N3
L'organisation doit classifier les informations conformément aux besoins de sécurité de l'information de l'organisation, sur la base des exigences de confidentialité, d'intégrité, de disponibilité et des exigences importantes des parties intéressées.		✓	✓

Objectif

Assurer l'identification et la compréhension des besoins de protection de l'information en fonction de son importance pour l'organisation.

6.5 Marquage des informations

Mesure de sécurité	N1	N2	N3
L'organisation doit élaborer et mettre en œuvre un ensemble approprié de procédures pour le marquage des informations, conformément au schéma de classification des informations adopté par l'organisation.		✓	✓

Objectif

Faciliter la communication de la classification de l'information et appuyer l'automatisation de la gestion et du traitement de l'information.

6.6 Gestion des supports de stockage

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre des procédures de gestion sécurisée des supports de stockage (disques durs, clés USB, etc.) pour toutes les phases de leur cycle de vie (acquisition, utilisation, transport, destruction), en fonction de la classification des informations qu'ils contiennent, incluant la suppression sécurisée ou le chiffrement.		✓	✓

Objectif

S'assurer que seul(e) la divulgation, la modification, le retrait ou la destruction autorisés des informations de l'organisation sur des supports de stockage sont effectués.

D7. Contrôle d'accès

7.1 Contrôle d'accès

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en place un processus de gestion du cycle de vie des identités numériques (création, modification, suspension,	✓	✓	✓

suppression) garantissant l'unicité de l'identité, la pertinence des attributs et la traçabilité des actions.			

Objectif

Permettre l'identification unique des personnes et des systèmes qui accèdent aux informations et autres actifs associés de l'organisation, et pour permettre l'attribution appropriée des droits d'accès.

7.2 Droits d'accès

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et mettre en œuvre des règles visant à contrôler l'accès physique et logique aux informations et autres actifs associés en fonction des exigences métier et de sécurité de l'information.	✓	✓	✓

Objectif

Assurer l'accès autorisé et empêcher l'accès non autorisé aux informations et autres actifs associés.

7.3 Gestion des identités

Mesure de sécurité	N1	N2	N3
L'organisation doit gérer le cycle de vie complet des identités en veillant à ce que les droits d'accès aux informations et autres actifs associés soient pourvus, révisés, modifiés et supprimés.	✓	✓	✓
L'organisation doit effectuer une revue semestrielle des droits d'accès.			✓

Objectif

Assurer que l'accès aux informations et autres actifs associés est défini et autorisé conformément aux exigences métier.

7.4 Droit d'accès privilégiés

Mesure de sécurité	N1	N2	N3
L'organisation doit limiter et gérer l'attribution et l'utilisation des droits d'accès privilégiés.	✓	✓	✓

Objectif

S'assurer que seuls les utilisateurs, composants logiciels et services autorisés sont dotés de droits d'accès privilégiés.

7.5 Informations d'authentification

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en place un processus de gestion des informations d'authentification telles que les identifiants et les mots de passe, et fournir au personnel des consignes claires pour leur utilisation sécurisée.	✓	✓	✓

Objectif

Assurer l'authentification correcte de l'entité et éviter les défaillances des processus d'authentification.

7.6 Restrictions d'accès aux informations

Mesure de sécurité	N1	N2	N3
L'organisation doit restreindre l'accès aux informations et autres actifs associés conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.	✓	✓	✓

Objectif

Assurer les accès autorisés seulement et empêcher les accès non autorisés aux informations et autres actifs associés.

7.7 Authentification sécurisée

Mesure de sécurité	N1	N2	N3
L'organisation doit implémenter des mécanismes d'authentification robustes, incluant si nécessaire l'authentification multi-facteurs (MFA) pour les accès sensibles, et renforcer les exigences de complexité et de renouvellement des informations d'authentification (mots de passe, certificats).		✓	✓

Objectif

S'assurer qu'un utilisateur ou une entité est authentifié(e) de façon sécurisée lorsque l'accès aux systèmes, applications et services lui est accordé.

7.8 Utilisation de programmes utilitaires à privilèges

Mesure de sécurité	N1	N2	N3
L'organisation doit limiter et contrôler étroitement l'utilisation de programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes et des applications.		✓	✓

Objectif

S'assurer que l'utilisation de programmes utilitaires ne nuise pas aux mesures de sécurité de l'information des systèmes et des applications.

7.9 Accès aux codes sources

Mesure de sécurité	N1	N2	N3
L'organisation doit gérer de manière appropriée l'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels.		✓	✓

Objectif

Empêcher l'introduction d'une fonctionnalité non autorisée, éviter les modifications non intentionnelles ou malveillantes et préserver la confidentialité de la propriété intellectuelle importante.

D8. Cryptographie

8.1 Utilisation de la cryptographie

Mesure de sécurité	N1	N2	N3
L'organisation doit établir une politique cryptographique documentée, spécifiant les algorithmes, les longueurs de clés et les protocoles à utiliser, et implémenter une gestion rigoureuse du cycle de vie des clés cryptographiques (génération, stockage, distribution, révocation, destruction) pour protéger la confidentialité et l'intégrité des informations.		✓	✓

Objectif

Assurer l'utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité, l'authenticité ou l'intégrité des informations conformément aux exigences métier et de sécurité de l'information, et en tenant compte des exigences légales, statutaires, réglementaires et contractuelles relatives à la cryptographie.

D9. Sécurité physique et environnementale

9.1 Périmètre de sécurité physique

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et utiliser des périmètres de sécurité pour protéger les zones qui contiennent les informations et autres actifs associés.		✓	✓

Objectif

Empêcher l'accès physique non autorisé, les dommages ou interférences portant sur les informations et autres actifs associés de l'organisation.

9.2 Les entrées physiques

Mesure de sécurité	N1	N2	N3
L'organisation doit protéger les zones sécurisées par des mesures de sécurité des accès et des points d'accès appropriés.		✓	✓

Objectif

Assurer que seul l'accès physique autorisé aux informations et autres actifs associés de l'organisation soit possible.

9.3 Surveillance de la sécurité physique

Mesure de sécurité	N1	N2	N3
Les locaux de l'organisation doivent être continuellement gardés et surveillés pour empêcher l'accès physique non autorisé.		✓	✓

Objectif

Détecter et dissuader l'accès physique non autorisé.

9.4 Sécurisation des bureaux, des salles et des installations

Mesure de sécurité	N1	N2	N3
L'organisation doit concevoir et mettre en œuvre des mesures de sécurité physique pour les bureaux, les salles et les installations.	✓	✓	✓

Objectif

Empêcher l'accès physique non autorisé, les dommages et les interférences impactant les informations et autres actifs associés de l'organisation dans les bureaux, salles et installations.

9.5 Protection contre les menaces physiques et environnementales

Mesure de sécurité	N1	N2	N3
L'organisation doit identifier et évaluer les risques physiques et environnementaux et mettre en œuvre des mesures de protection adéquates pour les zones contenant des informations et actifs critiques.	✓	✓	✓

Objectif

Prévenir ou réduire les conséquences des événements issus des menaces physiques ou environnementales.

9.6 Travail dans les zones sécurisées

Mesure de sécurité	N1	N2	N3
L'organisation doit s'assurer que les mesures de sécurité pour le travail dans les zones sécurisées soient conçues et mises en œuvre.		✓	✓

Objectif

Protéger les informations et autres actifs associés dans les zones sécurisées contre tout dommage et contre toutes interférences non autorisées par le personnel travaillant dans ces zones.

9.7 Emplacement et protection du matériel

Mesure de sécurité	N1	N2	N3
L'organisation doit choisir un emplacement sécurisé pour le matériel et le protéger.	✓	✓	✓

Objectif

Réduire les risques liés à des menaces physiques et environnementales, à des accès non autorisés et à des dommages.

9.8 Services supports

Mesure de sécurité	N1	N2	N3
L'organisation doit protéger les moyens de traitement de l'information contre les coupures d'électricité et autres perturbations causées par des défaillances des services supports.		✓	✓

Objectif

Empêcher la perte, l'endommagement ou la compromission des informations et autres actifs associés, ou l'interruption des activités de l'organisation, causés par les défaillances et les perturbations des services supports.

9.9 Sécurité du câblage

Mesure de sécurité	N1	N2	N3
L'organisation doit protéger les câbles électriques ou de télécommunication, transportant des données ou supportant les services d'information contre les interceptions, les interférences ou les dommages.	✓	✓	✓

Objectif

Empêcher la perte, l'endommagement, le vol ou la compromission des informations et autres actifs associés et l'interruption des activités de l'organisation liés au câblage électrique et de télécommunication.

9.10 Maintenance du matériel

Mesure de sécurité	N1	N2	N3
L'organisation doit entretenir le matériel correctement pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.	✓	✓	✓

Objectif

Empêcher la perte, l'endommagement, le vol ou la compromission des informations et autres actifs associés et l'interruption des activités de l'organisation causés par un manque de maintenance.

9.11 Supports de stockage

Mesure de sécurité	N1	N2	N3
L'organisation doit gérer les supports de stockage tout au long de leur cycle de vie (acquisition, utilisation, transport et mise au rebut) conformément au schéma de classification et aux exigences de traitement de l'organisation.		✓	✓

Objectif

S'assurer que seul(e) la divulgation, la modification, le retrait ou la destruction autorisés des informations de l'organisation sur des supports de stockage sont effectués.

9.12 Sécurité des actifs hors des locaux

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre des mesures de sécurité appliquées aux matériels utilisés hors des locaux, en tenant compte des différents risques associés au travail hors site.		✓	✓

Objectif

Empêcher la perte, l'endommagement, le vol ou la compromission des terminaux hors du site et l'interruption des activités de l'organisation.

9.13 Mise au rebut du matériel

Mesure de sécurité	N1	N2	N3
L'organisation doit vérifier tout matériel mise au rebut contenant des supports de stockage pour s'assurer que toute donnée sensible a été supprimé et tout logiciel sous licence a été désinstallé de manière sécurisée, avant son élimination ou sa réutilisation.		✓	✓

Objectif

Éviter la fuite d'informations à partir de matériel à éliminer ou à réutiliser.

9.14 Bureau propre et écran vide

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et appliquer de manière appropriée des règles de rangements claires pour les documents papier et les supports de stockage amovibles, ainsi que des règles d'écran vide pour les moyens de traitement de l'information.	✓	✓	✓

Objectif

Réduire les risques d'accès non autorisé, de perte et d'endommagement des informations sur les bureaux, les écrans et dans d'autres emplacements accessibles pendant et en dehors des heures normales de travail.

D10. Sécurité liée à l'exploitation

10.1 Procédures d'exploitation documentées

Mesure de sécurité	N1	N2	N3
L'organisation doit s'assurer que les procédures d'exploitation des moyens de traitement de l'information sont documentées et mises à disposition du personnel qui en a besoin.		✓	✓

Objectif

S'assurer du fonctionnement correct et sécurisé des moyens de traitement de l'information.

10.2 Gestion des configurations

Mesure de sécurité	N1	N2	N3
L'organisation doit, définir, documenter, mettre en œuvre, surveiller et réviser les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux.	✓	✓	✓

Objectif

S'assurer que le matériel, les logiciels, les services et les réseaux fonctionnent correctement avec les paramètres de sécurité requis, et que la configuration n'est pas altérée par des changements non autorisés ou incorrects.

10.3 Dimensionnement

Mesure de sécurité	N1	N2	N3
L'organisation doit surveiller l'utilisation des ressources et ajuster selon les besoins de dimensionnement actuels prévus.	✓	✓	✓

Objectif

Assurer les besoins en termes de moyens de traitement de l'information, de ressources humaines, de bureaux et autres installations.

10.4 Protection contre les programmes malveillants

Mesure de sécurité	N1	N2	N3
L'organisation doit déployer et maintenir à jour des solutions de protection contre les programmes malveillants et sensibiliser de façon continue les utilisateurs aux menaces émergentes.	✓	✓	✓

Objectif

S'assurer que les informations et autres actifs associés sont protégés contre les programmes malveillants.

10.5 Filtrage web

Mesure de sécurité	N1	N2	N3
L'organisation doit contrôler l'accès des utilisateurs aux sites web pour réduire l'exposition aux contenus malveillants.	✓	✓	✓

Objectif

Protéger les systèmes contre la compromission des programmes malveillants et empêcher l'accès aux ressources web non autorisées.

10.6 Prévention de la fuite de données

Mesure de sécurité	N1	N2	N3
L'organisation doit appliquer aux systèmes des mesures de prévention de fuite de données, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.	✓	✓	✓

Objectif

Détecter et empêcher la divulgation et l'extraction non autorisées d'informations par des personnes ou des systèmes.

10.7 Sauvegarde des informations

Mesure de sécurité	N1	N2	N3
L'organisation doit conserver et tester régulièrement des copies de sauvegarde de l'information, des logiciels et des systèmes selon la politique de sauvegarde qui a été convenue.	✓	✓	✓

Objectif

Permettre la récupération en cas de perte de données ou de systèmes.

10.8 Suppression sécurisée des informations

Mesure de sécurité	N1	N2	N3
L'organisation doit supprimer de manière sécurisée, lorsqu'elles ne sont plus nécessaires, les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage.	✓	✓	✓

Objectif

Empêcher l'exposition inutile des informations sensibles et se conformer aux exigences légales, statutaires, réglementaires et contractuelles relatives à la suppression d'informations.

10.9 Journalisation

Mesure de sécurité	N1	N2	N3
Les journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents doivent être générés, conservés, protégés et analysés.	✓	✓	✓

Objectif

Enregistrer les événements, générer des preuves, assurer l'intégrité des informations de journalisation, empêcher les accès non autorisés, identifier les événements de sécurité de l'information qui peuvent engendrer un incident et assister les investigations.

10.10 Activités de surveillance

Mesure de sécurité	N1	N2	N3
L'organisation doit surveiller les réseaux, systèmes et applications pour détecter les comportements anormaux et prendre des mesures appropriées.		✓	✓

Objectif

Détecter les comportements anormaux et évaluer les éventuels incidents de sécurité de l'information.

10.11 Synchronisation des horloges

Mesure de sécurité	N1	N2	N3
Les horloges des systèmes de traitement de l'information utilisées par l'organisation doivent être synchronisées avec des sources de temps approuvées.	✓	✓	✓

Objectif

Permettre la corrélation et l'analyse d'événements de sécurité et autres données enregistrées, assister les investigations sur les incidents de sécurité de l'information.

10.12 Installation de logiciels sur des systèmes opérationnels

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre des procédures et des mesures pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels.	✓	✓	✓

Objectif

Assurer l'intégrité des systèmes opérationnels.

10.13 Gestion des vulnérabilités techniques

Mesure de sécurité	N1	N2	N3
L'organisation doit établir un processus continu de gestion des vulnérabilités.		✓	✓

Objectif

Empêcher l'exploitation des vulnérabilités techniques.

10.14 Protection des systèmes d'information pendant les tests d'audit

Mesure de sécurité	N1	N2	N3
L'organisation doit planifier et valider avec les parties prenantes les exigences et activités d'audit des systèmes en exploitation.		✓	✓

Objectif

Minimiser l'impact des activités d'audit et autres activités d'assurance sur les systèmes opérationnels et les processus métier.

D11. Sécurité des communications

11.1 Sécurité des réseaux

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre une architecture réseau sécurisée pour protéger les informations et les systèmes contre les accès non autorisés et les attaques réseaux.		✓	✓

Objectif

Protéger les informations dans les réseaux et les moyens de traitement de l'information support contre les compromissions via le réseau.

11.2 Sécurité des services réseaux

Mesure de sécurité	N1	N2	N3
L'organisation doit identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et les intégrer dans les accords avec les fournisseurs de services réseau en interne ou externalisés.			✓

Objectif

Assurer la sécurité lors de l'utilisation des services réseau.

11.3 Cloisonnement des réseaux

Mesure de sécurité	N1	N2	N3
Les groupes de services d'information et d'utilisateurs doivent être cloisonnés dans les réseaux de l'organisation.		✓	✓

Objectif

Diviser le réseau en périmètres de sécurité et contrôler le trafic entre eux en fonction des besoins métier.

11.4 Transfert des informations

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en place des règles, procédures ou accords sur le transfert des informations pour tous les types de moyens de transfert au sein de l'organisation, et entre l'organisation et des tierces parties.		✓	✓

Objectif

Maintenir la sécurité de l'information transférée au sein de l'organisation et vers toute partie intéressée externe.

11.5 Accords de confidentialité ou de non-divulgation

Mesure de sécurité	N1	N2	N3
L'organisation doit s'assurer que les accords de confidentialité ou de non-divulgation représentant les besoins de l'organisation relatifs à la protection des informations soient identifiés, documentés, régulièrement révisés et signés par le personnel et les autres parties intéressées.	✓	✓	✓

Objectif

Assurer la confidentialité des informations accessibles par le personnel ou les parties externes.

D12. Acquisition, développement et maintenance des systèmes d'information

12.1 Sécurité de l'information dans la gestion de projet

Mesure de sécurité	N1	N2	N3
L'organisation doit intégrer la sécurité de l'information dans la gestion de projet.		✓	✓

Objectif

S'assurer que les risques de sécurité de l'information relatifs aux projets et aux livrables sont traités efficacement dans la gestion de projet, tout au long du cycle de vie du projet.

12.2 Exigences de sécurité des applications

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et approuver des exigences de sécurité de l'information lors du développement ou de l'acquisition d'applications.		✓	✓

Objectif

S'assurer que toutes les exigences de sécurité de l'information sont identifiées et traitées lors du développement ou de l'acquisition d'applications.

12.3 Cycle de vie de développement sécurisé

Mesure de sécurité	N1	N2	N3
L'organisation doit intégrer la sécurité à chaque étape du cycle de vie de développement des logiciels et des systèmes, depuis la conception, l'implémentation, jusqu'au déploiement et à la maintenance, en utilisant des pratiques de développement sécurisé reconnues.		✓	✓

Objectif

S'assurer que la sécurité de l'information est conçue et mise en œuvre au cours du cycle de vie de développement sécurisé des logiciels et des systèmes.

12.4 Codage sécurisé

Mesure de sécurité	N1	N2	N3
L'organisation doit appliquer des principes de codage sécurisé au développement de logiciels.		✓	✓

Objectif

S'assurer que les logiciels sont développés de manière sécurisée afin de réduire le nombre d'éventuelles vulnérabilités de sécurité de l'information dans les logiciels.

12.5 Gestion des changements

Mesure de sécurité	N1	N2	N3
Les changements apportés aux moyens de traitement de l'information et aux systèmes d'information doivent être soumis à des procédures de gestion des changements.		✓	✓

Objectif

Préserver la sécurité de l'information lors de l'exécution des changements.

12.6 Principes d'ingénierie et d'architecture des systèmes sécurisés

Mesure de sécurité	N1	N2	N3
L'organisation doit établir, documenter, tenir à jour et appliquer à toutes les activités de développement de systèmes d'information, des principes d'ingénierie des systèmes sécurisés.		✓	✓

Objectif

S'assurer que les systèmes d'information sont conçus, mis en œuvre et exploités de manière sécurisée au cours du cycle de vie de développement.

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

Mesure de sécurité	N1	N2	N3
L'organisation doit séparer et sécuriser les environnements de développement, de test et d'exploitation.		✓	✓

Objectif

Protéger l'environnement opérationnel et les données correspondantes contre les compromissions qui pourraient être dues aux activités de développement et de test.

12.8 Développement externalisé

Mesure de sécurité	N1	N2	N3
L'organisation doit diriger, contrôler et vérifier les activités relatives au développement externalisé des systèmes.		✓	✓

Objectif

S'assurer que les mesures de sécurité de l'information requises par l'organisation sont mises en œuvre dans le cadre du développement externalisé des systèmes.

12.9 Informations de test

Mesure de sécurité	N1	N2	N3
L'organisation doit sélectionner, protéger et gérer de manière appropriée les informations de test.	✓	✓	✓

Objectif

Assurer la pertinence des tests et la protection des informations opérationnelles utilisées.

12.10 Masquage des données

Mesure de sécurité	N1	N2	N3
L'organisation doit utiliser le masquage des données conformément à la politique de contrôle d'accès de l'organisation et aux autres politiques spécifiques à une thématique associée, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.		✓	✓

Objectif

Limiter l'exposition des données sensibles, y compris les DCP, et se conformer aux exigences légales, statutaires, réglementaires et contractuelles.

D13. Relations avec les fournisseurs

13.1 La sécurité de l'information dans les accords conclus avec les fournisseurs

Mesure de sécurité	N1	N2	N3
L'organisation doit intégrer des clauses de sécurité de l'information claires et détaillées dans tous les contrats avec les fournisseurs, spécifiant les exigences de sécurité, les obligations de conformité, les droits d'audit, et les responsabilités en cas d'incident de sécurité.	✓	✓	✓

Objectif

Maintenir le niveau de sécurité de l'information convenu dans les relations avec les fournisseurs.

13.2 Sécurité de l'information dans l'utilisation de services cloud

Mesure de sécurité	N1	N2	N3
L'organisation doit établir conformément à ses exigences de sécurité de l'information, les processus d'acquisition, d'utilisation, de gestion et de cessation des services cloud.		✓	✓

Objectif

Spécifier et gérer la sécurité de l'information lors de l'utilisation de services cloud.

13.3 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC

Mesure de sécurité	N1	N2	N3
L'organisation doit définir et mettre en œuvre des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC.		✓	✓

Objectif

Maintenir le niveau de sécurité de l'information convenu dans les relations avec les fournisseurs.

13.4 Surveillance, révision et gestion des changements des services fournisseurs

Mesure de sécurité	N1	N2	N3
L'organisation doit procéder régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et des prestations de services.	✓	✓	✓

Objectif

Maintenir un niveau convenu de sécurité de l'information et des prestations de services, conformément aux accords conclus avec les fournisseurs.

D14. Gestion des incidents de sécurité de l'information

14.1 Planification et préparation de la gestion des incidents de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit établir un Plan de Réponse aux Incidents (PRI) en procédant à la définition, à l'établissement et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de sécurité de l'information.		✓	✓
L'organisation doit mettre en place un système de traitement des incidents, transmettre les relevés techniques à l'ANSSI et les conserver pendant une période minimum de 6 mois.			✓

Objectif

Assurer une réponse rapide, efficace, cohérente et ordonnée aux incidents de sécurité de l'information, notamment la communication sur les événements de sécurité de l'information.

14.2 Déclaration des événements de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit fournir un mécanisme au personnel pour déclarer rapidement les événements de sécurité de l'information observés ou suspectés, à travers des canaux appropriés.		✓	✓
L'organisation doit mettre en place des moyens techniques de détection des incidents, définir une procédure formalisée de traitement des alertes et déclarer immédiatement tout incident à l'ANSSI.			✓

Objectif

Permettre la déclaration des événements de sécurité de l'information qui peuvent être identifiés par le personnel, de manière rapide, cohérente et efficace.

14.3 Évaluation des événements de sécurité de l'information et prise de décision

Mesure de sécurité	N1	N2	N3
L'organisation doit évaluer les événements de sécurité de l'information et décider s'ils doivent être catégorisés comme des incidents de sécurité de l'information.		✓	✓

Objectif

Assurer une catégorisation et une priorisation efficaces des événements de sécurité de l'information.

14.4 Réponse aux incidents de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit répondre aux incidents de sécurité de l'information conformément aux procédures documentées.		✓	✓

Objectif

Assurer une réponse efficace et effective aux incidents de sécurité de l'information.

14.5 Tirer des enseignements des incidents de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit utiliser les connaissances acquises à partir des incidents de sécurité de l'information pour renforcer et améliorer les mesures de sécurité de l'information.		✓	✓

Objectif

Réduire la probabilité ou les conséquences des incidents futurs.

14.6 Collecte des preuves

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en place des procédures d'investigation numérique (forensic) pour les événements de sécurité, garantissant l'intégrité et l'authenticité des éléments collectés à des fins d'investigation interne, disciplinaire ou judiciaire.		✓	✓

Objectif

Assurer une gestion cohérente et efficace des preuves relatives aux incidents de sécurité de l'information pour les besoins d'actions judiciaires et/ou disciplinaires.

D15. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

15.1 Sécurité de l'information pendant une perturbation

Mesure de sécurité	N1	N2	N3
L'organisation doit planifier le niveau approprié du maintien de la sécurité de l'information pendant une perturbation.		✓	✓

Objectif

Protéger les informations et autres actifs associés pendant une perturbation.

15.2 Redondance des moyens de traitement de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit assurer la redondance des moyens de traitement de l'information afin de maintenir la disponibilité des services.		✓	✓

Objectif

S'assurer du fonctionnement continu des moyens de traitement de l'information.

15.3 Préparation des TIC pour la continuité d'activité

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre des plans de reprise d'activité (PRA) et de continuité d'activité (PCA) régulièrement testés, afin de minimiser l'impact des perturbations.		✓	✓
L'organisation doit mettre le PCA à disposition de l'ANSSI.			✓

Objectif

Assurer la disponibilité des informations et autres actifs associés de l'organisation pendant une perturbation.

D16. Conformité

16.1 Exigences légales, statutaires, réglementaires et contractuelles

Mesure de sécurité	N1	N2	N3
L'organisation doit recenser l'ensemble des exigences légales, réglementaires, statutaires et contractuelles relatives à la sécurité de l'information, et définir une approche documentée pour en assurer la conformité.	✓	✓	✓

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires et contractuelles relatives à la sécurité de l'information.

16.2 Droits de propriété intellectuelle

Mesure de sécurité	N1	N2	N3
L'organisation doit mettre en œuvre les procédures appropriées pour protéger les droits de propriété intellectuelle.	✓	✓	✓

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de produits propriétaires.

16.3 Protection des enregistrements

Mesure de sécurité	N1	N2	N3
L'organisation doit protéger les enregistrements à minima contre la perte, la destruction, la falsification, les accès et les diffusions non autorisées.	✓	✓	✓

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires et contractuelles, ainsi qu'aux attentes de la société ou de la communauté relatives à la protection et à la disponibilité des enregistrements.

16.4 Protection de la vie privée et des données à caractère personnel

Mesure de sécurité	N1	N2	N3
L'organisation doit identifier et respecter les exigences relatives à la protection de la vie privée et des DCP conformément aux lois, réglementations et exigences contractuelles applicables.	✓	✓	✓

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires et contractuelles relatives aux aspects de la sécurité de l'information portant sur la protection des DCP.

16.5 Révision interne de la sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit réaliser en interne une évaluation de son dispositif de gestion de la sécurité de l'information, couvrant les dimensions humaines, procédurales et technologiques, selon une périodicité planifiée ou en cas de changement majeur.		✓	✓

Objectif

S'assurer que l'approche de l'organisation pour gérer la sécurité de l'information est continuellement adaptée, adéquate et efficace.

16.6 Conformité aux politiques, règles et normes de sécurité de l'information

Mesure de sécurité	N1	N2	N3
L'organisation doit s'assurer que la conformité à la politique de sécurité de l'information, aux politiques spécifiques à une thématique, aux règles et aux normes de l'organisation est régulièrement vérifiée.	✓	✓	✓
L'organisation doit commanditer un audit de sécurité du système d'information par un PASSI agréé ANSSI et lui transmettre le rapport.			✓

Objectif

S'assurer que la sécurité de l'information est mise en œuvre et fonctionne conformément à la politique de sécurité de l'information, aux politiques spécifiques à une thématique, aux règles et aux normes de l'organisation.

GLOSSAIRE

ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information. Autorité nationale en charge de la cybersécurité.

AIPD

Analyse d'Impact relative à la Protection des Données. Évaluation des risques liés aux traitements de données personnelles.

Authentification

Processus permettant de vérifier l'identité d'un utilisateur, d'un système ou d'un service.

Codage sécurisé

Ensemble de pratiques de développement visant à éviter les vulnérabilités dans le code source.

Confidentialité

Propriété d'une information qui n'est accessible qu'aux personnes autorisées.

Cycle de vie de développement

Ensemble des phases par lesquelles passe un logiciel, de sa conception à sa mise hors service.

Classification des informations

Processus de catégorisation des informations en fonction de leur sensibilité et de leur criticité.

Cloud

Services en nuage qui désignent l'accès à des ressources informatiques (stockage des données, serveurs, logiciels…) via internet.

DCP

Données à Caractère Personnel. Informations permettant d'identifier directement ou indirectement une personne physique.

DLP

Data Loss Prevention. Technologies et politiques visant à prévenir la fuite de données.

DPO

Correspondant à la Protection des Données (Data Protection Officer). Responsable de la conformité à la loi relative à la protection des données à caractère personnel.

EDR

Endpoint Detection and Response. Outil de détection et de réponse aux menaces sur les postes de travail.

Forensique numérique

Ensemble des techniques et méthodes utilisées pour collecter, analyser et préserver des preuves numériques.

Filtrage web

Contrôle de l'accès aux sites Internet selon des règles de sécurité définies.

Gestion des configurations

Processus de définition, de suivi et de contrôle des paramètres des systèmes et logiciels.

Gestion des vulnérabilités

Processus de détection, d'évaluation et de traitement des vulnérabilités dans les systèmes d'information.

Incident de sécurité

Événement compromettant la confidentialité, l'intégrité ou la disponibilité des informations.

Journalisation

Enregistrement des événements et activités dans les systèmes d'information.

Masquage des données

Technique de protection des données consistant à remplacer les valeurs sensibles par des données fictives.

MFA

Multi-Factor Authentication. Authentification à plusieurs facteurs (ex. mot de passe + code SMS).

PASSI

Prestataire d'Audit de Sécurité des Systèmes de l'Information

PSSI

Politique de Sécurité des Systèmes d'Information. Document définissant les orientations stratégiques en matière de sécurité.

PRA

Plan de Reprise d'Activité. Ensemble de procédures pour restaurer les services après un incident majeur.

PRI

Plan de Réponse aux Incidents. Ensemble de procédures pour répondre efficacement aux incidents de sécurité.

Programme utilitaire à privilèges

Logiciel ou outil disposant de droits d'accès élevés, permettant l'exécution d'actions critiques sur les systèmes d'information.

PCA

Plan de Continuité d'Activité. Ensemble de mesures pour assurer la continuité des activités critiques.

RGSSI

Référentiel Général de Sécurité des Systèmes d'Information. Cadre normatif national pour la sécurité des SI.

RSSI

Responsable de la Sécurité des Systèmes d'Information. Personne en charge de la mise en œuvre de la politique de sécurité.

SI

Système d'Information. Ensemble structuré de ressources (matériels, logiciels, données, procédures) permettant de collecter, traiter, stocker et diffuser de l'information.

SSI

Sécurité des Systèmes d'Information.

TIC

Technologies de l'Information et de la Communication. Ensemble des technologies utilisées pour le traitement et la transmission de l'information.

Vulnérabilité

Faiblesse dans un système pouvant être exploitée pour compromettre sa sécurité.

Redondance

Duplication des composants ou fonctions critiques d'un système pour augmenter sa fiabilité.

Synchronisation des horloges

Processus visant à aligner les horloges des différents systèmes pour assurer la cohérence des événements enregistrés.