Système de management de la sécurité de l'information

# Politique Générale de Sécurité des Systèmes d'Information

| Référence | Référence | Date |
| --- | --- | --- |
| | | 29/05/2025 |

## 1. Informations Générales

| Item | Valeur |
| --- | --- |
| Type de politique | SSI |
| Statut | Applicable |
| Périmètre d'application | Ensemble des systèmes, données, utilisateurs, partenaires et prestataires intervenant dans le cadre des activités numériques de D&A Technologies, y compris les environnements cloud et les sites distants. |
| Rédacteur | El Mahdi Mouline |
| Valideur | Khalid Benlyazid El Hassani |
| Date d'approbation | 29 Mai 2025 |
| Date d'entrée en vigueur | 29 Mai 2025 |

## 2. Contexte et Justification

La présente Politique Générale de Sécurité des Systèmes d'Information (PGSSI) est élaborée dans le but d'établir un cadre de référence pour la protection des actifs informationnels de l'ensemble du département IT de D&A TECHNOLOGIES. Conscients des risques croissants et de la criticité des systèmes d'information dans l'atteinte des objectifs stratégiques de l'organisation, il est impératif de définir et de mettre en œuvre des directives claires et des mesures de sécurité robustes. Cette politique constitue la première version (1.0), marquant une étape initiale dans la formalisation et l'amélioration continue de notre posture de sécurité.

## 3. Objectifs de la Politique SSI

Cette politique vise à :

- Assurer la confidentialité des informations traitées et stockées par les systèmes d'information de D&A TECHNOLOGIES.
- Garantir l'intégrité des données contre toute modification non autorisée ou erreur.
- Maintenir la disponibilité des services et des informations pour les utilisateurs autorisés en cas de besoin.
- Définir les responsabilités de chaque acteur en matière de sécurité des systèmes d'information.
- Fournir un cadre pour la mise en œuvre et le suivi des mesures de sécurité.
- Se conformer aux exigences légales et réglementaires applicables en matière de sécurité de l'information.
- Sensibiliser et former le personnel aux bonnes pratiques de sécurité.
- Établir un processus de gestion des incidents de sécurité.

## 4. Périmètre d'Application

La présente politique s'applique à l'ensemble des infrastructures, des systèmes, des applications, des réseaux, des données et des utilisateurs du département IT de D&A TECHNOLOGIES**,** qu'ils soient internes ou externes, et quel que soit leur emplacement physique ou logique. Elle concerne également les prestataires et les partenaires ayant accès aux systèmes d'information de D&A TECHNOLOGIES.

## 5. Évolutions Futures

Cette version 1.0 de la Politique PGSSI servira de base pour les développements futurs. Des révisions et des mises à jour régulières seront effectuées afin de prendre en compte l'évolution des menaces, des technologies et des besoins de l'organisation. Les prochaines versions pourront inclure des détails plus spécifiques sur les différentes aspects de la sécurité, tels que le contrôle d'accès, la gestion des mots de passe, la sécurité du réseau, la protection contre les logiciels malveillants, la sauvegarde et la restauration des données, et la gestion des incidents de sécurité.

# SOMMAIRE

1. Le mot du Directeur Général 5

2. Introduction 7

2.1 Objectif de la PGSSI 7

2.2 Champ d'application 7

2.3 Références 7

3. Politique de Sécurité 8

3.1 Engagement de la Direction 8

3.2 Objectifs de Sécurité 8

4. Organisation des Contrôles de Sécurité (Annexe A.5) 10

4.1 5.1 Politiques de Sécurité de l'Information 10

4.2 5.2 Responsabilités en Matière de Sécurité de l'Information 10

4.3 5.3 Séparation des Tâches 10

4.4 5.4 Responsabilités de la Direction 10

4.5 5.5 Contact avec les Autorités 10

4.6 5.6 Contact avec des Groupes d'Intérêt Spécial 11

4.7 5.7 Renseignement sur les Menaces 11

4.8 5.8 Sécurité de l'Information dans la Gestion de Projets 11

4.9 5.9 Inventaire des Informations et des Actifs Associés 11

4.10 5.11 Retour des Actifs 11

4.11 5.12 Classification de l'Information 11

4.12 5.13 Étiquetage de l'Information 12

4.13 5.14 Transfert de l'Information 12

4.14 5.15 Contrôle d'Accès 12

4.15 5.16 Gestion des Identités 12

4.16 5.17 Information d'Authentification 12

4.17 5.18 Droits d'Accès 12

4.18 5.19 Sécurité de l'Information dans les Relations avec les Fournisseurs 13

4.19 5.20 Prise en Compte de la Sécurité de l'Information dans les Contrats Fournisseurs 13

4.20 5.21 Gestion de la Sécurité de l'Information dans la Chaîne d'Approvisionnement TIC 13

4.21 5.22 Surveillance, Revue et Gestion des Changements des Services Fournis 13

4.22 5.23 Sécurité de l'Information pour l'Utilisation des Services Cloud 13

4.23 5.24 Planification et Préparation à la Gestion des Incidents de Sécurité de l'Information 13

4.24 5.25 Évaluation et Décision sur les Événements de Sécurité de l'Information 14

4.25 5.26 Réponse aux Incidents de Sécurité de l'Information 14

4.26 5.27 Apprentissage des Incidents de Sécurité de l'Information 14

4.27 5.28 Collecte de Preuves 14

4.28 5.29 Sécurité de l'Information en Cas de Perturbation 14

4.29 5.30 Préparation des TIC à la Continuité des Activités 15

4.30 5.31 Identification des Exigences Légales, Statutaires, Réglementaires et Contractuelles 15

4.31 5.32 Droits de Propriété Intellectuelle 15

4.32 5.33 Protection des Documents 15

4.33 5.34 Confidentialité et Protection des Données Personnelles (PII) 15

4.34 5.35 Revue Indépendante de la Sécurité de l'Information 15

4.35 5.36 Conformité aux Politiques et Normes de Sécurité de l'Information 16

4.36 5.37 Procédures Opérationnelles Documentées 16

5. Contrôles des Personnes (Annexe A.6) 17

5.1 6.1 Vérification (Screening) 17

5.2 6.2 Termes et Conditions d'Emploi (Terms and Conditions of Employment) 17

5.3 6.3 Sensibilisation, Éducation et Formation à la Sécurité de l'Information (Information Security Awareness and Education ) 17

5.4 6.4 Processus Disciplinaire (Disciplinary Process) 17

5.5 6.5 Responsabilités après la Fin ou le Changement d'Emploi (Responsibilities After Termination or Change of Employment) 17

5.6 6.6 Accords de Confidentialité ou de Non-Divulgation (Confidentiality or Non-Disclosure Agreements) 17

5.7 6.7 Télétravail (Remote Working) 18

5.8 6.8 Signalement des Événements de Sécurité de l'Information (Information Security Event Reporting) 18

6. Contrôles Physiques (Annexe A.7) 19

6.1 7.1 Périmètre de Sécurité Physique (Physical Security Perimeter) 19

6.2 7.2 Contrôles d'Entrée Physique (Physical Entry Controls) 19

6.3 7.3 Sécurisation des Bureaux, Salles et Installations (Securing Offices, Rooms and Facilities) 19

6.4 7.4 Surveillance de la Sécurité Physique (Physical Security Monitoring) 19

6.5 7.5 Protection contre les Menaces Physiques et Environnementales (Protecting Against Physical and Environmental Threats) 19

6.6 7.6 Travailler dans des Zones Sécurisées (Working in Secure Areas) 19

6.7 7.7 Politique de Bureau Propre et Écran Propre (Clear Desk and Clear Screen) 20

6.8 7.8 Emplacement et Protection des Équipements (Equipment Siting and Protection) 20

6.9 7.9 Sécurité des Actifs Hors des Locaux (Security of Assets Off-Premises) 20

6.10 7.10 Supports de Stockage (Storage Media) 20

6.11 7.11 Utilitaires de Support (Supporting Utilities) 20

6.12 7.12 Sécurité des Câblages (Cabling Security) 20

6.13 7.13 Maintenance des Équipements (Equipment Maintenance) 21

6.14 7.14 Élimination ou Réutilisation Sécurisée des Équipements (Secure Disposal or Re-Use of Equipment) 21

7. Contrôles Technologiques (Annexe A.8) 22

7.1 8.1 Dispositifs d'Extrémité des Utilisateurs (User Endpoint Devices) 22

7.2 8.2 Droits d'Accès Privilégiés (Privileged Access Rights) 22

7.3 8.3 Restriction de l'Accès à l'Information (Information Access Restriction) 22

7.4 8.4 Accès au Code Source (Access to Source Code) 22

7.5 8.5 Authentification Sécurisée (Secure Authentication) 22

7.6 8.6 Gestion de la Capacité (Capacity Management) 23

7.7 8.7 Protection contre les Logiciels Malveillants (Protection Against Malware) 23

7.8 8.8 Gestion des Vulnérabilités Techniques (Management of Technical Vulnerabilities) 23

7.9 8.9 Gestion de la Configuration (Configuration Management) 23

7.10 8.10 Suppression des Informations (Information Deletion) 23

7.11 8.11 Masquage des Données (Data Masking) 24

7.12 8.12 Prévention des Fuites de Données (Data Leakage Prevention) 24

7.13 8.13 Sauvegarde de l'Information (Information Backup) 24

7.14 8.14 Redondance des Installations de Traitement de l'Information (Redundancy of Information Processing Facilities) 24

7.15 8.15 Journaux (Logging) 24

7.16 8.16 Surveillance des Activités (Monitoring Activities) 25

7.17 8.17 Synchronisation des Horloges (Clock Synchronisation) 25

7.18 8.18 Utilisation des Programmes Utilitaires Privilégiés (Use of Privileged Utility Programs) 25

7.19 8.19 Installation de Logiciels sur les Systèmes Opérationnels (Installation of Software on Operational Systems) 25

7.20 8.20 Contrôles Réseau (Network Controls) 25

7.21 8.21 Sécurité des Services Réseau (Security of Network Services) 26

7.22 8.22 Ségrégation dans les Réseaux (Segregation in Networks) 26

7.23 8.23 Filtrage Web (Web Filtering) 26

7.24 8.24 Utilisation de la Cryptographie (Use of Cryptography) 26

7.25 8.25 Cycle de Vie du Développement Sécurisé (Secure Development Lifecycle) 26

7.26 8.26 Exigences de Sécurité des Applications (Application Security Requirements) 27

7.27 8.27 Principes de Conception et d'Ingénierie des Systèmes Sécurisés (Secure System Architecture and Engineering Principles) 27

7.28 8.29 Tests de Sécurité dans le Développement et l'Acceptation (Security Testing in Development and Acceptance) 27

7.29 8.30 Développement Externalisé (Outsourced Development) 27

7.30 8.31 Séparation des Environnements de Développement, de Test et de Production (Separation of Development, Test and Production Environments) 27

7.31 8.32 Gestion des Changements (Change Management) 28

7.32 8.33 Informations de Test (Test Information) 28

7.33 8.34 Protection des Systèmes d'Information pendant les Audits et les Tests (Protection of Information Systems During Audit and Testing) 28

# 1. Le mot du Directeur Général

Opérant dans un environnement de plus en plus ouvert et confronté à une augmentation des menaces de toute nature, le D&A TECHNOLOGIES vient d'entamer depuis plusieurs mois une réflexion sur la protection de son patrimoine humain, informationnel et matériel.

Les enjeux sont vitaux, tant vis-à-vis de nos clients, dont nous nous sommes engagés à protéger les intérêts, que vis-à-vis de notre établissement, dont il est essentiel de préserver l'image de marque et la réputation.

Dans cette perspective, D&A TECHNOLOGIES considère primordial que ses actifs soient protégés efficacement. L'absence de protection adéquate pourrait affecter le rendement de D&A TECHNOLOGIES et porter atteinte à son image ainsi qu'à la confiance que lui accordent ses partenaires.

Dans ce contexte, et afin de poursuivre les démarches déjà engagées, D&A TECHNOLOGIES a décidé de renforcer cette politique sécuritaire comme un thème majeur et stratégique pour les années à venir. D&A TECHNOLOGIES attire l'attention de l'ensemble des acteurs et des collaborateurs, quel que soit leur niveau hiérarchique, au rôle qu'ils ont à jouer dans ce sens.

Des principes de sécurité ont été élaborés et décrits dans ce document afin que les décisions D&A TECHNOLOGIES reposent sur des informations fiables, accessibles de façon sécuritaire et dont la confidentialité aura été préservée. Ces principes devront être respectés par l'ensemble du personnel et seront étroitement surveillés.

La sécurité étant l'affaire de tous, la stratégie mise en œuvre implique un effort constant de chacun et le respect d'un certain nombre de directives internes et de règles de sécurité.

**M. Driss Lahrichi**

**Directeur Général**

# PRÉSENTATION DE LA POLITIQUE DE SÉCURITÉ

L'information étant une valeur essentielle dans la conduite des activités, elle représente une ressource stratégique pour D&A TECHNOLOGIES. La sécurité du système d'information est un élément essentiel du management de l'information au sein de D&A TECHNOLOGIES.

La sécurité du système d'information couvre l'ensemble des mesures de prévention, de correction et de détection mises en œuvre pour réduire ou éliminer les risques et les conséquences d'actions ou d'événements, internes ou externes, volontaires, involontaires ou accidentels, qui pourraient porter atteinte à la Disponibilité, à l'Intégrité, à la Confidentialité et à la Preuve (Traçabilité) des informations « **DICP** ».

**Contenu de la Politique de Sécurité du Système d'Information**

La Politique de Sécurité du Système d'Information contient le message du Directeur Général, les orientations de D&A TECHNOLOGIES en matière de sécurité du système d'information et les règles de conduite applicables par l'ensemble des collaborateurs de D&A TECHNOLOGIES pour protéger l'information et les actifs informationnels.

Elle a pour objet de définir :

- Le cadre général d'organisation dans le domaine de la sécurité du système information
- Les éléments structurants de la sécurité du système d'information qui traitent des principes d'architecture, de la sécurité logique et de la sécurité physique
- Les règles générales à mettre en œuvre par tous les utilisateurs de l'information, et par le management
- Les règles spécifiques concernant la sécurisation des informations et, plus précisément, l'exploitation de l'infrastructure informatique ; le contrôle d'accès ; l'acquisition, le développement et la maintenance des systèmes d'information, la sécurité physique et environnementale, la gestion des incidents, la continuité d'activités et la conformité aux législations.
- Les moyens de pilotage de la sécurité à tous les niveaux.

# 2. Introduction

## 2.1 Objectif de la PGSSI

- **Définition des Objectifs** : La politique de sécurité des systèmes d'information (PGSSI) a pour objectif de protéger les actifs informationnels de l'entreprise contre les menaces internes et externes. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations.
- **Alignement Stratégique** : La PGSSI doit être alignée avec les objectifs stratégiques de l'entreprise, en soutenant la continuité des opérations et en minimisant les risques de sécurité.
- **Responsabilisation** : Définir les responsabilités de chaque employé et des parties prenantes en matière de sécurité de l'information. Chaque membre de l'organisation doit comprendre son rôle dans la protection des informations.

## 2.2 Champ d'application

- **Portée Organisationnelle** : La PGSSI s'applique à l'ensemble des entités de l'entreprise, incluant tous les départements, unités opérationnelles et filiales.
- **Portée Technologique** : Inclure tous les systèmes d'information, applications, réseaux, bases de données et dispositifs utilisés au sein de l'entreprise.
- **Portée Géographique** : La politique couvre toutes les installations de l'entreprise, y compris les bureaux distants, les sites de production et les centres de données situés à l'étranger.
- **Groupes Ciblés** : S'applique à tous les employés, prestataires, consultants et autres parties prenantes ayant accès aux informations et systèmes de l'entreprise.

## 2.3 Références

- **Normes et Réglementations** : La PGSSI doit être conforme aux normes ISO/IEC 27001:2022 ainsi qu'aux autres normes pertinentes telles que ISO/IEC 27002:2022.
- **Législations Nationales et Internationales** : Se conformer aux lois et réglementations en matière de protection des données et de la vie privée, telles que la loi 09-08 et la RGPD.

# 3. Politique de Sécurité

## 3.1 Engagement de la Direction

- **Déclaration d'Engagement** : La direction de l'entreprise s'engage fermement à soutenir et promouvoir la sécurité de l'information à tous les niveaux de l'organisation.
  - La direction doit établir une déclaration officielle de son engagement en matière de sécurité de l'information, incluant la protection des actifs informationnels contre toutes formes de menaces.
  - Cette déclaration doit être communiquée à tous les employés, prestataires et parties prenantes pour garantir une compréhension et un alignement clairs des objectifs de sécurité.
- **Ressources Allouées** : La direction s'engage à allouer les ressources nécessaires pour assurer la mise en œuvre efficace de la politique de sécurité de l'information.
  - Les ressources incluent des budgets, des technologies, du personnel formé et des processus adaptés pour gérer la sécurité de l'information.
  - Des investissements réguliers doivent être faits pour mettre à jour les systèmes de sécurité et former le personnel.
- **Responsabilité de la Sécurité** : La direction définit clairement les rôles et responsabilités en matière de sécurité de l'information.
  - Les responsabilités de sécurité doivent être intégrées dans les descriptions de poste et les évaluations de performance.
  - Un responsable de la sécurité de l'information (RSI) doit être désigné pour superviser et coordonner les activités de sécurité.
- **Culture de Sécurité** : La direction promeut une culture de sécurité au sein de l'organisation.
  - Des programmes de sensibilisation et de formation à la sécurité de l'information doivent être développés et mis en œuvre régulièrement.
  - La direction doit encourager la communication ouverte concernant les incidents de sécurité et les risques potentiels.

## 3.2 Objectifs de Sécurité

- **Définition des Objectifs** : Établir des objectifs clairs, mesurables et réalisables pour la sécurité de l'information.
  - Les objectifs doivent être alignés avec les risques identifiés, les exigences légales et réglementaires, et les besoins opérationnels de l'entreprise.
  - Les objectifs doivent inclure des indicateurs de performance pour mesurer l'efficacité des contrôles de sécurité.
- **Revue et Mise à Jour des Objectifs** : Les objectifs de sécurité doivent être régulièrement revus et mis à jour pour refléter les changements dans l'environnement de menace et les priorités de l'entreprise.
  - Une revue annuelle des objectifs de sécurité doit être réalisée pour s'assurer qu'ils restent pertinents et alignés avec la stratégie de l'entreprise.
  - Les résultats des revues doivent être documentés et communiqués à la direction et aux parties prenantes concernées.
- **Intégration dans les Processus d'Affaires** : Les objectifs de sécurité doivent être intégrés dans les processus d'affaires et les projets de l'entreprise.
  - Les projets doivent inclure des étapes spécifiques pour évaluer et intégrer les exigences de sécurité.
  - Les processus opérationnels doivent être conçus pour minimiser les risques de sécurité et assurer la conformité continue avec les objectifs de sécurité.
- **Évaluation de la Conformité** : Les objectifs de sécurité doivent inclure des mécanismes d'évaluation de la conformité pour vérifier l'adhérence aux politiques et procédures de sécurité.

- Des audits internes et externes doivent être réalisés régulièrement pour évaluer la conformité aux objectifs de sécurité.
- Les écarts identifiés doivent être corrigés rapidement et efficacement pour améliorer la posture de sécurité de l'entreprise.

# 4. Organisation des Contrôles de Sécurité (Annexe A.5)

## 4.1 5.1 Politiques de Sécurité de l'Information

- **DOC-PSI-01** : La politique de sécurité de l'information doit être développée en prenant en compte les besoins de l'entreprise, les risques identifiés, les exigences légales et les objectifs de sécurité.
- **DOC-PSI-02** : Les politiques doivent être rédigées avec clarté, précision et applicabilité, couvrant tous les aspects critiques de la sécurité de l'information.
- **DOC-PSI-03** : Les politiques doivent être approuvées par la Direction Générale avant leur diffusion.
- **DOC-PSI-04** : Les politiques approuvées doivent être publiées et diffusées auprès de tous les employés et des tiers concernés. Des sessions de formation et de sensibilisation doivent être organisées pour expliquer les politiques de sécurité et leur importance.
- **DOC-PSI-05** : Les politiques doivent être accessibles sur l'intranet de l'entreprise et sur d'autres plateformes de communication internes.

## 4.2 5.2 Responsabilités en Matière de Sécurité de l'Information

- **DOC-PSI-06** : Les rôles et responsabilités en matière de sécurité de l'information doivent être clairement définis pour tous les employés, incluant les administrateurs système, les utilisateurs finaux, et le responsable de la sécurité de l'information (RSI).
- **DOC-PSI-07** : Les descriptions de poste doivent inclure des responsabilités spécifiques en matière de sécurité de l'information.
- **DOC-PSI-08** : Un organigramme de la sécurité de l'information doit être créé pour montrer les lignes de responsabilité et de rapport.

## 4.3 5.3 Séparation des Tâches

- **DOC-PSI-09** : La séparation des tâches doit être mise en œuvre pour réduire les risques d'erreurs ou d'activités frauduleuses.
- **DOC-PSI-10** : Les fonctions critiques ne doivent pas être exercées par une seule personne sans une supervision appropriée.
- **DOC-PSI-11** : Des contrôles internes doivent être mis en place pour vérifier le respect de la séparation des tâches.

## 4.4 5.4 Responsabilités de la Direction

- **DOC-PSI-12** : La direction doit démontrer son engagement en matière de sécurité de l'information en allouant les ressources nécessaires et en soutenant les initiatives de sécurité.
- **DOC-PSI-13** : Des réunions régulières doivent être organisées entre la direction et les responsables de la sécurité pour discuter des problèmes de sécurité.
- **DOC-PSI-14** : La direction doit encourager une culture de la sécurité au sein de l'entreprise.

## 4.5 5.5 Contact avec les Autorités

- **DOC-PSI-15** : Des procédures doivent être établies pour maintenir des contacts appropriés avec les autorités réglementaires et autres autorités concernées.

- **DOC-PSI-16** : Un point de contact principal doit être désigné pour les communications avec les autorités.

## 4.6 5.6 Contact avec des Groupes d'Intérêt Spécial

- **DOC-PSI-17** : Maintenir des contacts avec des groupes d'intérêt spécial ou des forums pour se tenir informé des menaces de sécurité actuelles et des bonnes pratiques.
- **DOC-PSI-18** : Encourager la participation active aux groupes et forums de sécurité de l'information.

## 4.7 5.7 Renseignement sur les Menaces

- **DOC-PSI-19** : Des processus doivent être mis en place pour collecter et analyser des informations sur les menaces potentielles afin de renforcer la posture de sécurité.
- **DOC-PSI-20** : Les renseignements sur les menaces doivent être régulièrement mis à jour et communiqués aux parties prenantes pertinentes.

## 4.8 5.8 Sécurité de l'Information dans la Gestion de Projets

- **DOC-PSI-21** : La sécurité de l'information doit être intégrée dans la gestion de projets pour garantir que les contrôles de sécurité sont pris en compte dès le début du projet.
- **DOC-PSI-22** : Des évaluations de sécurité doivent être réalisées à chaque étape critique du projet.
- **DOC-PSI-23** : Les projets doivent inclure des plans de sécurité spécifiques et des ressources dédiées à la gestion de la sécurité.

## 4.9 5.9 Inventaire des Informations et des Actifs Associés

- **DOC-PSI-24** : Un inventaire complet des informations et des actifs associés doit être maintenu pour assurer une gestion appropriée et sécurisée.
- **DOC-PSI-25** : Les actifs doivent être classifiés et étiquetés en fonction de leur sensibilité et de leur importance.
- **DOC-PSI-26** : Des audits réguliers de l'inventaire doivent être réalisés pour garantir son exactitude et sa mise à jour.

## 4.10 5.11 Retour des Actifs

- **DOC-PSI-30** : Des procédures doivent être mises en place pour garantir que tous les actifs de l'entreprise sont retournés lors de la cessation d'emploi ou de contrat.
- **DOC-PSI-31** : Les actifs doivent être inspectés pour vérifier leur état et s'assurer qu'aucune information sensible n'est présente.
- **DOC-PSI-32** : Les comptes d'accès associés doivent être désactivés et les accès révoqués.

## 4.11 5.12 Classification de l'Information

- **DOC-PSI-33** : Les informations doivent être classifiées en fonction de leur sensibilité et de leur importance pour garantir une protection adéquate.
- **DOC-PSI-34** : Des niveaux de classification standard doivent être définis et appliqués de manière cohérente à travers l'entreprise.

- **DOC-PSI-35** : Des formations doivent être dispensées pour aider les employés à comprendre et appliquer correctement les classifications.

## 4.12 5.13 Étiquetage de l'Information

- **DOC-PSI-36** : Des procédures d'étiquetage doivent être mises en place pour identifier clairement le niveau de classification de chaque information.
- **DOC-PSI-37** : Les étiquettes doivent être visibles et conformes aux politiques de classification de l'entreprise.
- **DOC-PSI-38** : Des contrôles réguliers doivent être effectués pour s'assurer que les informations sont correctement étiquetées.

## 4.13 5.14 Transfert de l'Information

- **DOC-PSI-39** : Des contrôles doivent être mis en œuvre pour protéger les informations lors de leur transfert, que ce soit par des moyens physiques ou électroniques.
- **DOC-PSI-40** : Les transferts d'informations sensibles doivent être chiffrés et effectués via des canaux sécurisés.
- **DOC-PSI-41** : Des politiques et des procédures doivent être établies pour garantir que les transferts d'information sont autorisés et suivis.

## 4.14 5.15 Contrôle d'Accès

- **DOC-PSI-42** : Les contrôles d'accès doivent être établis pour garantir que seules les personnes autorisées peuvent accéder aux informations et aux systèmes.
- **DOC-PSI-43** : Les droits d'accès doivent être accordés en fonction des rôles et des responsabilités des utilisateurs.
- **DOC-PSI-44** : Des audits réguliers des accès doivent être effectués pour vérifier leur conformité.

## 4.15 5.16 Gestion des Identités

- **DOC-PSI-45** : Des processus de gestion des identités doivent être mis en place pour gérer l'attribution et la révocation des droits d'accès.
- **DOC-PSI-46** : Les identités des utilisateurs doivent être vérifiées et validées avant l'octroi des accès.
- **DOC-PSI-47** : Un registre centralisé des identités doit être maintenu et régulièrement mis à jour.

## 4.16 5.17 Information d'Authentification

- **DOC-PSI-48** : Des mesures doivent être prises pour protéger les informations d'authentification contre les accès non autorisés.
- **DOC-PSI-49** : Les informations d'authentification doivent être stockées de manière sécurisée, utilisant des techniques de hachage et de chiffrement.
- **DOC-PSI-50** : Les politiques de gestion des mots de passe doivent inclure des exigences sur la complexité, la durée de vie et le changement régulier des mots de passe.

## 4.17 5.18 Droits d'Accès

- **DOC-PSI-51** : Les droits d'accès doivent être attribués en fonction des responsabilités et révoqués en cas de changement de rôle ou de départ.
- **DOC-PSI-52** : Un processus formel de demande et d'approbation des accès doit être établi.
- **DOC-PSI-53** : Les accès inutilisés doivent être désactivés pour réduire les risques de compromission.

## 4.18 5.19 Sécurité de l'Information dans les Relations avec les Fournisseurs

- **DOC-PSI-54** : Les fournisseurs doivent être évalués et gérés pour garantir qu'ils respectent les exigences de sécurité de l'entreprise.
- **DOC-PSI-55** : Des audits de sécurité réguliers doivent être effectués chez les fournisseurs critiques.
- **DOC-PSI-56** : Des clauses de sécurité doivent être incluses dans tous les contrats avec les fournisseurs.

## 4.19 5.20 Prise en Compte de la Sécurité de l'Information dans les Contrats Fournisseurs

- **DOC-PSI-57** : Les contrats avec les fournisseurs doivent inclure des clauses spécifiques de sécurité de l'information.
- **DOC-PSI-58** : Les obligations de sécurité doivent être clairement définies et les responsabilités de chaque partie doivent être documentées.
- **DOC-PSI-59** : Des mécanismes de surveillance doivent être établis pour assurer la conformité des fournisseurs.

## 4.20 5.21 Gestion de la Sécurité de l'Information dans la Chaîne d'Approvisionnement TIC

- **DOC-PSI-60** : Des contrôles doivent être mis en place pour gérer la sécurité de l'information dans la chaîne d'approvisionnement des TIC.
- **DOC-PSI-61** : Les fournisseurs TIC doivent être régulièrement évalués et surveillés pour garantir leur conformité aux exigences de sécurité.
- **DOC-PSI-62** : Les risques liés à la chaîne d'approvisionnement doivent être identifiés et atténués.

## 4.21 5.22 Surveillance, Revue et Gestion des Changements des Services Fournis

- **DOC-PSI-63** : La surveillance et la revue des services fournis par les fournisseurs doivent être effectuées régulièrement pour garantir leur conformité aux exigences de sécurité.
- **DOC-PSI-64** : Les changements dans les services fournis doivent être gérés de manière formelle pour évaluer et minimiser les impacts sur la sécurité.
- **DOC-PSI-65** : Des rapports de performance et de conformité doivent être régulièrement obtenus des fournisseurs.

## 4.22 5.23 Sécurité de l'Information pour l'Utilisation des Services Cloud

- **DOC-PSI-66** : Des mesures spécifiques doivent être mises en place pour assurer la sécurité de l'information lors de l'utilisation des services cloud.
- **DOC-PSI-67** : Les fournisseurs de services cloud doivent être évalués pour leur capacité à protéger les données et à respecter les exigences de sécurité.

- **DOC-PSI-68** : Des accords de niveau de service (SLA) doivent inclure des clauses de sécurité spécifiques pour les services cloud.

## 4.23 5.24 Planification et Préparation à la Gestion des Incidents de Sécurité de l'Information

- **DOC-PSI-69** : Un plan de gestion des incidents doit être élaboré et testé régulièrement pour garantir une réponse efficace en cas d'incident de sécurité.
- **DOC-PSI-70** : Les rôles et responsabilités en matière de gestion des incidents doivent être clairement définis et communiqués.
- **DOC-PSI-71** : Des exercices de simulation d'incidents doivent être réalisés pour tester l'efficacité des plans de réponse aux incidents.

## 4.24 5.25 Évaluation et Décision sur les Événements de Sécurité de l'Information

- **DOC-PSI-72** : Tous les événements de sécurité de l'information doivent être évalués et des décisions appropriées doivent être prises pour atténuer les risques.
- **DOC-PSI-73** : Un processus formel doit être établi pour la classification et la priorisation des événements de sécurité.
- **DOC-PSI-74** : Les réponses aux événements doivent être documentées et analysées pour améliorer les processus de gestion des incidents.

## 4.25 5.26 Réponse aux Incidents de Sécurité de l'Information

- **DOC-PSI-75** : Des procédures de réponse aux incidents doivent être mises en place pour traiter efficacement les incidents de sécurité de l'information.
- **DOC-PSI-76** : Les incidents doivent être signalés immédiatement et traités selon les procédures établies.
- **DOC-PSI-77** : Les actions correctives et préventives doivent être mises en œuvre pour éviter la récurrence des incidents.

## 4.26 5.27 Apprentissage des Incidents de Sécurité de l'Information

- **DOC-PSI-78** : Les incidents de sécurité de l'information doivent être analysés pour en tirer des leçons et améliorer les contrôles de sécurité.
- **DOC-PSI-79** : Des rapports post-incident doivent être rédigés et partagés avec les parties prenantes pertinentes.
- **DOC-PSI-80** : Les processus de gestion des incidents doivent être continuellement améliorés en fonction des leçons apprises.

## 4.27 5.28 Collecte de Preuves

- **DOC-PSI-81** : Des procédures doivent être mises en place pour collecter et préserver les preuves en cas d'incident de sécurité de l'information.
- **DOC-PSI-82** : Les preuves doivent être collectées de manière légale et conforme aux normes de sécurité.
- **DOC-PSI-83** : Les preuves doivent être stockées de manière sécurisée et accessibles uniquement aux personnes autorisées.

## 4.28 5.29 Sécurité de l'Information en Cas de Perturbation

- **DOC-PSI-84** : Des mesures doivent être prises pour garantir la sécurité de l'information pendant les perturbations des activités.
- **DOC-PSI-85** : Les plans de continuité des activités doivent inclure des stratégies pour maintenir la sécurité de l'information.
- **DOC-PSI-86** : Des exercices réguliers de continuité des activités doivent être menés pour s'assurer que les mesures de sécurité sont efficaces pendant les perturbations.

## 4.29 5.30 Préparation des TIC à la Continuité des Activités

- **DOC-PSI-87** : Les systèmes TIC doivent être préparés pour assurer la continuité des activités en cas de perturbation.
- **DOC-PSI-88** : Les systèmes critiques doivent être identifiés et des plans de redondance doivent être mis en place.
- **DOC-PSI-89** : Les systèmes TIC doivent être régulièrement testés pour vérifier leur capacité à maintenir les opérations pendant une perturbation.

## 4.30 5.31 Identification des Exigences Légales, Statutaires, Réglementaires et Contractuelles

- **DOC-PSI-90** : Toutes les exigences légales, statutaires, réglementaires et contractuelles pertinentes doivent être identifiées et respectées.
- **DOC-PSI-91** : Un registre des exigences légales et réglementaires doit être maintenu et régulièrement mis à jour.
- **DOC-PSI-92** : Les processus de conformité doivent être intégrés dans les opérations quotidiennes de l'entreprise.

## 4.31 5.32 Droits de Propriété Intellectuelle

- **DOC-PSI-93** : Les droits de propriété intellectuelle doivent être protégés et respectés.
- **DOC-PSI-94** : Des politiques doivent être mises en place pour gérer les droits de propriété intellectuelle, incluant la protection des marques, brevets et droits d'auteur.
- **DOC-PSI-95** : Les employés doivent être formés sur les exigences relatives à la propriété intellectuelle.

## 4.32 5.33 Protection des Documents

- **DOC-PSI-96** : Les documents contenant des informations sensibles doivent être protégés contre tout accès non autorisé.
- **DOC-PSI-97** : Les documents physiques doivent être stockés dans des emplacements sécurisés.
- **DOC-PSI-98** : Les documents électroniques doivent être protégés par des mesures de sécurité telles que le chiffrement et les contrôles d'accès.

## 4.33 5.34 Confidentialité et Protection des Données Personnelles (PII)

- **DOC-PSI-99** : Les données personnelles identifiables (PII) doivent être protégées conformément aux lois et réglementations sur la protection des données.
- **DOC-PSI-100** : Des politiques et procédures de confidentialité doivent être mises en place pour garantir la protection des PII.
- **DOC-PSI-101** : Les employés doivent être formés sur les exigences relatives à la confidentialité et à la protection des PII.

## 4.34 5.35 Revue Indépendante de la Sécurité de l'Information

- **DOC-PSI-102** : Des revues indépendantes de la sécurité de l'information doivent être réalisées régulièrement pour évaluer l'efficacité des contrôles.
- **DOC-PSI-103** : Les résultats des revues doivent être documentés et partagés avec la direction pour action.
- **DOC-PSI-104** : Des actions correctives doivent être mises en œuvre pour résoudre les faiblesses identifiées lors des revues.

## 4.35 5.36 Conformité aux Politiques et Normes de Sécurité de l'Information

- **DOC-PSI-105** : Tous les employés et les tiers doivent se conformer aux politiques et normes de sécurité de l'information de l'entreprise.
- **DOC-PSI-106** : Des audits de conformité doivent être effectués régulièrement pour vérifier le respect des politiques de sécurité.
- **DOC-PSI-107** : Les non-conformités identifiées doivent être corrigées rapidement pour garantir la sécurité continue des informations.

## 4.36 5.37 Procédures Opérationnelles Documentées

- **DOC-PSI-108** : Toutes les procédures opérationnelles doivent être documentées et mises à jour régulièrement pour garantir leur pertinence et leur efficacité.
- **DOC-PSI-109** : Les procédures documentées doivent être accessibles aux employés concernés et incluses dans les programmes de formation.
- **DOC-PSI-110** : Les changements aux procédures opérationnelles doivent être gérés formellement pour assurer une communication efficace et une mise en œuvre appropriée.

# 5. Contrôles des Personnes (Annexe A.6)

## 5.1 6.1 Vérification (Screening)

- **DOC-PSI-39** : Les antécédents des candidats doivent être vérifiés avant l'embauche pour s'assurer qu'ils sont fiables et aptes à accéder aux informations sensibles de l'entreprise.
- **DOC-PSI-40** : La vérification doit inclure des contrôles des références, des qualifications et des antécédents judiciaires, conformément aux exigences légales et réglementaires.

## 5.2 6.2 Termes et Conditions d'Emploi (Terms and Conditions of Employment)

- **DOC-PSI-41** : Les contrats de travail doivent inclure des clauses spécifiques relatives à la sécurité de l'information, stipulant les responsabilités des employés en matière de protection des informations de l'entreprise.
- **DOC-PSI-42** : Les employés doivent être informés de leurs obligations en matière de sécurité de l'information dès leur embauche.

## 5.3 6.3 Sensibilisation, Éducation et Formation à la Sécurité de l'Information (Information Security Awareness, Education and Training)

- **DOC-PSI-43** : Des programmes de sensibilisation, d'éducation et de formation à la sécurité de l'information doivent être mis en place pour tous les employés.
- **DOC-PSI-44** : Les formations doivent être régulières et couvrir les politiques de sécurité, les procédures et les meilleures pratiques pour protéger les informations de l'entreprise.

## 5.4 6.4 Processus Disciplinaire (Disciplinary Process)

- **DOC-PSI-45** : Un processus disciplinaire doit être établi pour traiter les violations des politiques de sécurité de l'information.
- **DOC-PSI-46** : Les employés doivent être informés des sanctions possibles en cas de non-respect des politiques de sécurité.

## 5.5 6.5 Responsabilités après la Fin ou le Changement d'Emploi (Responsibilities After Termination or Change of Employment)

- **DOC-PSI-47** : Des procédures doivent être mises en place pour révoquer les accès et récupérer les actifs de l'entreprise lors de la cessation ou du changement d'emploi.
- **DOC-PSI-48** : Un entretien de sortie doit être réalisé pour rappeler aux employés leurs obligations continues de confidentialité.

## 5.6 6.6 Accords de Confidentialité ou de Non-Divulgation (Confidentiality or Non-Disclosure Agreements)

- **DOC-PSI-49** : Les employés doivent signer des accords de confidentialité ou de non-divulgation pour protéger les informations sensibles de l'entreprise.
- **DOC-PSI-50** : Ces accords doivent rester en vigueur après la fin de l'emploi.

## 5.7 6.7 Télétravail (Remote Working)

- **DOC-PSI-51** : Des politiques spécifiques doivent être mises en place pour sécuriser le télétravail, incluant des mesures pour protéger les informations et les systèmes utilisés hors des locaux de l'entreprise.
- **DOC-PSI-52** : Les employés en télétravail doivent être formés aux pratiques de sécurité spécifiques au travail à distance.

## 5.8 6.8 Signalement des Événements de Sécurité de l'Information (Information Security Event Reporting)

- **DOC-PSI-53** : Une procédure de signalement des incidents de sécurité de l'information doit être établie pour permettre aux employés de signaler rapidement tout incident ou événement suspect.
- **DOC-PSI-54** : Les employés doivent être formés sur la procédure de signalement et encouragés à signaler tout événement de sécurité sans crainte de représailles.

# 6. Contrôles Physiques (Annexe A.7)

## 6.1 7.1 Périmètre de Sécurité Physique (Physical Security Perimeter)

- **DOC-PSI-55** : Des mesures de protection physique doivent être mises en place pour sécuriser les périmètres des installations, incluant des contrôles d'accès, des systèmes de surveillance et des gardes de sécurité.
- **DOC-PSI-56** : Des barrières physiques, telles que des clôtures et des portails, doivent être installées pour restreindre l'accès aux zones sensibles.

## 6.2 7.2 Contrôles d'Entrée Physique (Physical Entry Controls)

- **DOC-PSI-57** : Les accès aux bâtiments doivent être contrôlés à l'aide de badges d'identification et de systèmes de contrôle d'accès électronique.
- **DOC-PSI-58** : Les visiteurs doivent être enregistrés et accompagnés par du personnel autorisé lorsqu'ils se trouvent dans les zones sensibles.

## 6.3 7.3 Sécurisation des Bureaux, Salles et Installations (Securing Offices, Rooms and Facilities)

- **DOC-PSI-59** : Les bureaux, salles et installations doivent être sécurisés pour empêcher l'accès non autorisé aux informations sensibles.
- **DOC-PSI-60** : Les portes et fenêtres doivent être équipées de dispositifs de verrouillage robustes.

## 6.4 7.4 Surveillance de la Sécurité Physique (Physical Security Monitoring)

- **DOC-PSI-61** : Des systèmes de surveillance doivent être mis en place pour surveiller les zones sensibles et détecter toute activité suspecte.
- **DOC-PSI-62** : Les enregistrements de surveillance doivent être conservés pendant une période définie et examinés régulièrement.

## 6.5 7.5 Protection contre les Menaces Physiques et Environnementales (Protecting Against Physical and Environmental Threats)

- **DOC-PSI-63** : Les équipements doivent être protégés contre les menaces environnementales telles que les incendies, les inondations, et les coupures de courant, en installant des dispositifs de protection adéquats (extincteurs, systèmes d'alimentation sans interruption).
- **DOC-PSI-64** : Les salles de serveurs et autres zones critiques doivent être équipées de systèmes de surveillance environnementale pour détecter les variations de température, d'humidité, et autres conditions susceptibles de compromettre la sécurité des équipements.

## 6.6 7.6 Travailler dans des Zones Sécurisées (Working in Secure Areas)

- **DOC-PSI-65** : Les zones sécurisées doivent être accessibles uniquement au personnel autorisé et soumis à des contrôles d'accès stricts.

- **DOC-PSI-66** : Les employés travaillant dans des zones sécurisées doivent être formés aux procédures de sécurité spécifiques à ces zones.

## 6.7 7.7 Politique de Bureau Propre et Écran Propre (Clear Desk and Clear Screen)

- **DOC-PSI-67** : Les employés doivent suivre une politique de bureau propre et d'écran propre pour s'assurer que les informations sensibles ne sont pas laissées sans surveillance.
- **DOC-PSI-68** : Les documents sensibles doivent être rangés dans des classeurs verrouillés et les écrans d'ordinateur doivent être verrouillés lorsqu'ils ne sont pas utilisés.

## 6.8 7.8 Emplacement et Protection des Équipements (Equipment Siting and Protection)

- **DOC-PSI-69** : Les équipements doivent être placés dans des endroits sécurisés et protégés contre les dommages accidentels ou intentionnels.
- **DOC-PSI-70** : Des protections physiques doivent être installées pour empêcher l'accès non autorisé aux équipements.

## 6.9 7.9 Sécurité des Actifs Hors des Locaux (Security of Assets Off-Premises)

- **DOC-PSI-71** : Les actifs de l'entreprise utilisés hors des locaux doivent être protégés par des mesures de sécurité adéquates pour prévenir les pertes ou les vols.
- **DOC-PSI-72** : Les employés utilisant des actifs hors des locaux doivent être formés sur les mesures de protection appropriées.

## 6.10 7.10 Supports de Stockage (Storage Media)

- **DOC-PSI-73** : Les supports de stockage doivent être protégés contre les accès non autorisés et les pertes de données.
- **DOC-PSI-74** : Des procédures de gestion des supports de stockage doivent être mises en place pour assurer leur sécurité tout au long de leur cycle de vie.

## 6.11 7.11 Utilitaires de Support (Supporting Utilities)

- **DOC-PSI-75** : Les utilitaires de support, tels que l'alimentation électrique et les systèmes de refroidissement, doivent être maintenus pour garantir le fonctionnement continu des équipements critiques.
- **DOC-PSI-76** : Des systèmes de secours doivent être disponibles pour les utilitaires critiques en cas de défaillance.

## 6.12 7.12 Sécurité des Câblages (Cabling Security)

- **DOC-PSI-77** : Les câblages réseau et de télécommunication doivent être protégés contre les interceptions et les dommages.
- **DOC-PSI-78** : Des conduits et des chemins de câbles sécurisés doivent être utilisés pour protéger les câblages sensibles.

## 6.13 7.13 Maintenance des Équipements (Equipment Maintenance)

- **DOC-PSI-79** : Les équipements doivent être maintenus régulièrement pour garantir leur bon fonctionnement et leur sécurité.
- **DOC-PSI-80** : Les procédures de maintenance doivent inclure des contrôles de sécurité pour s'assurer que les équipements ne sont pas compromis pendant la maintenance.

## 6.14 7.14 Élimination ou Réutilisation Sécurisée des Équipements (Secure Disposal or Re-Use of Equipment)

- **DOC-PSI-81** : Les équipements doivent être éliminés ou réutilisés de manière sécurisée pour garantir que les informations sensibles ne peuvent pas être récupérées.
- **DOC-PSI-82** : Des procédures doivent être mises en place pour effacer de manière sécurisée toutes les données des équipements avant leur élimination ou réutilisation.

# 7. Contrôles Technologiques (Annexe A.8)

## 7.1 8.1 Dispositifs d'Extrémité des Utilisateurs (User Endpoint Devices)

- **DOC-PSI-83** : Les dispositifs d'extrémité des utilisateurs doivent être configurés et sécurisés pour protéger contre les accès non autorisés et les logiciels malveillants.
- **DOC-PSI-84** : Des solutions antivirus et anti-malware doivent être installées et régulièrement mises à jour sur tous les dispositifs d'extrémité.
- **DOC-PSI-85** : Les utilisateurs doivent être formés sur les bonnes pratiques de sécurité pour l'utilisation des dispositifs d'extrémité.

## 7.2 8.2 Droits d'Accès Privilégiés (Privileged Access Rights)

- **DOC-PSI-86** : Les droits d'accès privilégiés doivent être limités aux utilisateurs autorisés et régulièrement révisés pour éviter tout accès non justifié.
- **DOC-PSI-87** : Les activités des utilisateurs ayant des accès privilégiés doivent être surveillées et enregistrées.
- **DOC-PSI-88** : Des procédures doivent être mises en place pour révoquer immédiatement les droits d'accès en cas de départ ou de changement de poste des utilisateurs.

## 7.3 8.3 Restriction de l'Accès à l'Information (Information Access Restriction)

- **DOC-PSI-89** : L'accès aux informations sensibles doit être restreint selon le principe du moindre privilège.
- **DOC-PSI-90** : Des contrôles d'accès doivent être mis en place pour garantir que seules les personnes autorisées peuvent accéder aux informations sensibles.
- **DOC-PSI-91** : Des audits réguliers doivent être réalisés pour vérifier la conformité des accès aux politiques de sécurité.

## 7.4 8.4 Accès au Code Source (Access to Source Code)

- **DOC-PSI-92** : L'accès au code source doit être strictement contrôlé et limité aux développeurs et administrateurs autorisés.
- **DOC-PSI-93** : Des audits réguliers doivent être effectués pour vérifier les accès et les modifications apportées au code source.
- **DOC-PSI-94** : Les modifications au code source doivent être approuvées et documentées pour assurer la traçabilité et la responsabilité.

## 7.5 8.5 Authentification Sécurisée (Secure Authentication)

- **DOC-PSI-95** : Des mécanismes d'authentification forte doivent être mis en place pour accéder aux systèmes et aux informations critiques.
- **DOC-PSI-96** : L'utilisation de l'authentification multi-facteurs (MFA) doit être encouragée pour renforcer la sécurité.

- **DOC-PSI-97** : Les informations d'authentification doivent être protégées contre toute divulgation ou compromission.

## 7.6 8.6 Gestion de la Capacité (Capacity Management)

- **DOC-PSI-98** : Les capacités des systèmes d'information doivent être surveillées et gérées pour assurer un fonctionnement efficace et éviter les surcharges.
- **DOC-PSI-99** : Des plans de capacité doivent être établis pour prévoir et répondre aux besoins futurs.
- **DOC-PSI-100** : Des évaluations régulières doivent être effectuées pour identifier les besoins en capacité et ajuster les ressources en conséquence.

## 7.7 8.7 Protection contre les Logiciels Malveillants (Protection Against Malware)

- **DOC-PSI-101** : Des mesures de protection contre les logiciels malveillants doivent être mises en place sur tous les systèmes d'information.
- **DOC-PSI-102** : Les signatures des logiciels de protection doivent être mises à jour régulièrement pour détecter les nouvelles menaces.
- **DOC-PSI-103** : Les incidents liés aux logiciels malveillants doivent être surveillés et analysés pour améliorer les mesures de protection.

## 7.8 8.8 Gestion des Vulnérabilités Techniques (Management of Technical Vulnerabilities)

- **DOC-PSI-104** : Un programme de gestion des vulnérabilités doit être mis en place pour identifier, évaluer et corriger les vulnérabilités des systèmes.
- **DOC-PSI-105** : Des scans réguliers de vulnérabilités doivent être effectués et des correctifs appliqués rapidement.
- **DOC-PSI-106** : Les systèmes doivent être surveillés en continu pour détecter les nouvelles vulnérabilités et y répondre efficacement.

## 7.9 8.9 Gestion de la Configuration (Configuration Management)

- **DOC-PSI-107** : Des procédures de gestion de la configuration doivent être établies pour contrôler les modifications apportées aux systèmes d'information.
- **DOC-PSI-108** : Les configurations doivent être documentées et régulièrement révisées pour s'assurer qu'elles restent sécurisées.
- **DOC-PSI-109** : Des audits de configuration doivent être réalisés pour vérifier la conformité aux politiques de sécurité.

## 7.10 8.10 Suppression des Informations (Information Deletion)

- **DOC-PSI-110** : Des procédures de suppression sécurisée des informations doivent être mises en place pour garantir que les données supprimées ne peuvent pas être récupérées.
- **DOC-PSI-111** : Les méthodes de suppression doivent être conformes aux exigences légales et réglementaires.
- **DOC-PSI-112** : Les suppressions doivent être documentées et vérifiées pour assurer leur efficacité.

## 7.11 8.11 Masquage des Données (Data Masking)

- **DOC-PSI-113** : Des techniques de masquage des données doivent être utilisées pour protéger les informations sensibles lorsqu'elles sont utilisées dans des environnements de test ou de développement.
- **DOC-PSI-114** : Les données masquées doivent conserver leur utilité tout en empêchant leur divulgation non autorisée.
- **DOC-PSI-115** : Les processus de masquage des données doivent être régulièrement révisés pour refléter les nouvelles menaces et techniques.

## 7.12 8.12 Prévention des Fuites de Données (Data Leakage Prevention)

- **DOC-PSI-116** : Des solutions de prévention des fuites de données doivent être mises en place pour détecter et empêcher la transmission non autorisée d'informations sensibles.
- **DOC-PSI-117** : Les politiques de prévention des fuites de données doivent être régulièrement mises à jour pour refléter les nouvelles menaces et techniques d'exfiltration.
- **DOC-PSI-118** : Les incidents de fuite de données doivent être surveillés et analysés pour améliorer les mesures de prévention.

## 7.13 8.13 Sauvegarde de l'Information (Information Backup)

- **DOC-PSI-119** : Des procédures de sauvegarde régulières doivent être mises en place pour garantir la récupération des informations en cas de perte ou de corruption.
- **DOC-PSI-120** : Les sauvegardes doivent être stockées dans des emplacements sécurisés et régulièrement testées pour vérifier leur intégrité.
- **DOC-PSI-121** : Les procédures de sauvegarde doivent inclure des mesures de protection contre les accès non autorisés et les compromissions.

## 7.14 8.14 Redondance des Installations de Traitement de l'Information (Redundancy of Information Processing Facilities)

- **DOC-PSI-122** : Des mesures de redondance doivent être mises en place pour assurer la disponibilité continue des installations de traitement de l'information en cas de défaillance.
- **DOC-PSI-123** : Les plans de redondance doivent inclure des tests réguliers pour s'assurer de leur efficacité.
- **DOC-PSI-124** : Les installations de traitement de l'information doivent être surveillées pour détecter et répondre aux défaillances rapidement.

## 7.15 8.15 Journaux (Logging)

- **DOC-PSI-125** : Les activités des systèmes d'information doivent être enregistrées dans des journaux pour permettre l'audit et la détection des anomalies.
- **DOC-PSI-126** : Les journaux doivent être protégés contre toute altération ou accès non autorisé.
- **DOC-PSI-127** : Les journaux doivent être régulièrement analysés pour identifier les incidents de sécurité et les tendances suspectes.

## 7.16 8.16 Surveillance des Activités (Monitoring Activities)

- **DOC-PSI-128** : Des mécanismes de surveillance doivent être mis en place pour détecter et réagir aux activités suspectes ou non autorisées sur les systèmes d'information.
- **DOC-PSI-129** : Les alertes de surveillance doivent être examinées et traitées rapidement pour atténuer les risques potentiels.
- **DOC-PSI-130** : Les activités de surveillance doivent être documentées et révisées régulièrement pour améliorer leur efficacité.

## 7.17 8.17 Synchronisation des Horloges (Clock Synchronisation)

- **DOC-PSI-131** : Les horloges des systèmes d'information doivent être synchronisées avec des sources de temps fiables pour garantir l'exactitude des enregistrements.
- **DOC-PSI-132** : La synchronisation doit être vérifiée régulièrement pour maintenir la précision.
- **DOC-PSI-133** : Les écarts de synchronisation doivent être corrigés rapidement pour éviter les erreurs de timing.

## 7.18 8.18 Utilisation des Programmes Utilitaires Privilégiés (Use of Privileged Utility Programs)

- **DOC-PSI-134** : L'utilisation des programmes utilitaires privilégiés doit être contrôlée et limitée aux utilisateurs autorisés.
- **DOC-PSI-135** : Les activités des programmes utilitaires doivent être enregistrées et surveillées.
- **DOC-PSI-136** : Des audits réguliers doivent être effectués pour s'assurer que les programmes utilitaires sont utilisés conformément aux politiques de sécurité.

## 7.19 8.19 Installation de Logiciels sur les Systèmes Opérationnels (Installation of Software on Operational Systems)

- **DOC-PSI-137** : L'installation de logiciels sur les systèmes opérationnels doit être contrôlée pour éviter l'introduction de logiciels non autorisés ou malveillants.
- **DOC-PSI-138** : Des procédures de validation et de test doivent être en place pour vérifier la sécurité des nouveaux logiciels avant leur déploiement.
- **DOC-PSI-139** : Les logiciels doivent être régulièrement mis à jour et maintenus pour corriger les vulnérabilités et améliorer la sécurité.

## 7.20 8.20 Contrôles Réseau (Network Controls)

- **DOC-PSI-140** : Des contrôles de sécurité doivent être mis en place pour protéger les réseaux contre les accès non autorisés et les attaques.
- **DOC-PSI-141** : Les réseaux doivent être segmentés pour limiter la portée des incidents de sécurité.
- **DOC-PSI-142** : Les équipements réseau doivent être configurés et maintenus selon les meilleures pratiques de sécurité.

## 7.21 8.21 Sécurité des Services Réseau (Security of Network Services)

- **DOC-PSI-143** : La sécurité des services réseau fournis par des tiers doit être évaluée et surveillée pour garantir qu'ils respectent les exigences de sécurité de l'entreprise.
- **DOC-PSI-144** : Des contrats avec les fournisseurs de services réseau doivent inclure des clauses de sécurité spécifiques.
- **DOC-PSI-145** : Les services réseau doivent être régulièrement testés et mis à jour pour maintenir leur sécurité.

## 7.22 8.22 Ségrégation dans les Réseaux (Segregation in Networks)

- **DOC-PSI-146** : Les réseaux doivent être segmentés pour isoler les systèmes critiques et limiter la propagation des incidents.
- **DOC-PSI-147** : Les politiques de segmentation doivent être régulièrement révisées et mises à jour.
- **DOC-PSI-148** : Des contrôles d'accès doivent être mis en place pour garantir que seules les personnes autorisées peuvent accéder aux segments de réseau sensibles.

## 7.23 8.23 Filtrage Web (Web Filtering)

- **DOC-PSI-149** : Des solutions de filtrage web doivent être mises en place pour protéger contre les sites malveillants et inappropriés.
- **DOC-PSI-150** : Les politiques de filtrage web doivent être régulièrement mises à jour pour refléter les nouvelles menaces.
- **DOC-PSI-151** : Les incidents liés aux sites web malveillants doivent être surveillés et analysés pour améliorer les mesures de filtrage.

## 7.24 8.24 Utilisation de la Cryptographie (Use of Cryptography)

- **DOC-PSI-152** : La cryptographie doit être utilisée pour protéger la confidentialité, l'intégrité et l'authenticité des informations sensibles.
- **DOC-PSI-153** : Les clés cryptographiques doivent être gérées de manière sécurisée tout au long de leur cycle de vie.
- **DOC-PSI-154** : Les algorithmes et les protocoles de cryptographie utilisés doivent être conformes aux standards reconnus internationalement.

## 7.25 8.25 Cycle de Vie du Développement Sécurisé (Secure Development Lifecycle)

- **DOC-PSI-155** : Des pratiques de développement sécurisé doivent être intégrées dans le cycle de vie du développement des logiciels pour garantir la sécurité des applications.
- **DOC-PSI-156** : Les développeurs doivent être formés aux principes de développement sécurisé et aux meilleures pratiques.
- **DOC-PSI-157** : Des évaluations de sécurité doivent être effectuées à chaque étape du développement pour identifier et corriger les vulnérabilités.

## 7.26 8.26 Exigences de Sécurité des Applications (Application Security Requirements)

- **DOC-PSI-158** : Les exigences de sécurité doivent être définies clairement pour toutes les applications dès le début de leur développement.
- **DOC-PSI-159** : Les exigences de sécurité doivent inclure des contrôles pour la gestion des accès, la protection des données et la résilience face aux attaques.
- **DOC-PSI-160** : Les exigences doivent être régulièrement mises à jour pour refléter l'évolution des menaces et des technologies.

## 7.27 8.27 Principes de Conception et d'Ingénierie des Systèmes Sécurisés (Secure System Architecture and Engineering Principles)

- **DOC-PSI-161** : Les systèmes doivent être conçus et développés en suivant des principes de sécurité robustes pour minimiser les risques.
- **DOC-PSI-162** : Des architectures de défense en profondeur doivent être mises en œuvre pour fournir plusieurs couches de protection.
- **DOC-PSI-163** : Les principes de sécurité doivent être intégrés dès la phase de conception et tout au long du cycle de vie des systèmes.

## 7.28 8.29 Tests de Sécurité dans le Développement et l'Acceptation (Security Testing in Development and Acceptance)

- **DOC-PSI-164** : Des tests de sécurité doivent être effectués pendant le développement et avant l'acceptation des systèmes pour identifier et corriger les vulnérabilités.
- **DOC-PSI-165** : Les tests de sécurité doivent inclure des analyses statiques et dynamiques du code, ainsi que des tests de pénétration.
- **DOC-PSI-166** : Les résultats des tests de sécurité doivent être documentés et les actions correctives doivent être suivies jusqu'à leur résolution.

## 7.29 8.30 Développement Externalisé (Outsourced Development)

- **DOC-PSI-167** : Les fournisseurs de développement externalisé doivent être évalués pour s'assurer qu'ils respectent les exigences de sécurité de l'entreprise.
- **DOC-PSI-168** : Les contrats avec les fournisseurs doivent inclure des clauses spécifiques de sécurité de l'information.
- **DOC-PSI-169** : Des audits réguliers doivent être réalisés pour vérifier la conformité des fournisseurs aux exigences de sécurité.

## 7.30 8.31 Séparation des Environnements de Développement, de Test et de Production (Separation of Development, Test and Production Environments)

- **DOC-PSI-170** : Les environnements de développement, de test et de production doivent être séparés pour prévenir les risques d'accès non autorisé et de modification des données.
- **DOC-PSI-171** : Des contrôles d'accès stricts doivent être mis en place pour chaque environnement.

- **DOC-PSI-172** : Les données de production ne doivent pas être utilisées dans les environnements de test ou de développement sans les protections appropriées.

## 7.31 8.32 Gestion des Changements (Change Management)

- **DOC-PSI-173** : Une procédure de gestion des changements doit être mise en place pour garantir que tous les changements aux systèmes d'information sont contrôlés et documentés.
- **DOC-PSI-174** : Les changements doivent être évalués pour leurs impacts potentiels sur la sécurité avant d'être mis en œuvre.
- **DOC-PSI-175** : Les changements doivent être approuvés par les parties prenantes pertinentes avant d'être déployés.

## 7.32 8.33 Informations de Test (Test Information)

- **DOC-PSI-176** : Les informations utilisées pour les tests doivent être protégées contre tout accès non autorisé et toute divulgation.
- **DOC-PSI-177** : Des mesures doivent être prises pour anonymiser ou masquer les données sensibles utilisées dans les environnements de test.
- **DOC-PSI-178** : Les informations de test doivent être gérées de manière sécurisée tout au long de leur cycle de vie.

## 7.33 8.34 Protection des Systèmes d'Information pendant les Audits et les Tests (Protection of Information Systems During Audit and Testing)

- **DOC-PSI-179** : Des mesures de protection doivent être mises en place pour garantir que les systèmes d'information ne sont pas compromis pendant les audits et les tests.
- **DOC-PSI-180** : Les activités d'audit et de test doivent être planifiées et coordonnées pour minimiser les risques pour les systèmes en production.
- **DOC-PSI-181** : Les résultats des audits et des tests doivent être traités de manière confidentielle et utilisés pour améliorer la sécurité des systèmes.