# JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

*N° 563 du 14 juin 2017*

**Règlement grand-ducal du 22 mai 2017 modifiant le règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.**

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la loi du 25 juillet 2015 relative à l'archivage électronique et notamment son article 4, paragraphe 1er;

Vu les avis de la Chambre de commerce et de la Chambre des métiers;

Notre Conseil d'État entendu;

Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil;

*Arrêtons:*

**Art. 1er.**

L'annexe du règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique est remplacée par l'annexe jointe au présent règlement grand-ducal.

**Art. 2.**

Notre Ministre de l'Économie est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

*Le Ministre de l'Économie,*
**Étienne Schneider**

Palais de Luxembourg, le 22 mai 2017.
**Henri**

# ANNEXE

## Règle technique pour un système de management et mesures de sécurité pour les Prestataires de Services de Dématérialisation ou de Conservation.

# Table des matières

**0 Introduction** 9
0.1 Contexte 9
0.2 Structure du document 9
**1 Domaine d'application** 11
**2 Références normatives** 12
**3 Termes et définitions** 13
3.1 actif 13
3.2 analogique 13
3.3 archive 14
3.4 archive numérique 14
3.5 authenticité 14
3.6 confidentialité 14
3.7 conservation (éléctronique) 14
3.8 dématérialisation 14
3.9 disponibilité 14
3.10 document 14
3.11 fiabilité 14
3.12 gestion 15
3.13 indexation 15
3.14 intégrité 15
3.15 métadonnées 15
3.16 non-répudiation 15
3.17 organisme 15
3.18 prestataire de services de dématerialisation ou de conservation (PSDC) 15
3.19 preuve 16
3.20 processus 16
3.21 sécurité de l'information 16
3.22 système 16
3.23 système de conservation 16
3.24 système de dématérialisation 16
3.25 système de dématérialisation ou de conservation (SDC) 16
**4 Exigences spécifiques pour PSDC et complémentaires à la norme ISO/IEC 27001:2013** 17
4.1 Structure de ce standard 17
4.2 Exigences spécifiques aux systèmes de management des PSDC 17

4 Contexte de l'organisation 17
4.0 Système de Management des processus de dématérialisation ou de conservation 17
4.3 Détermination du domaine d'applicabilité 17
4.5 L'authenticité, la fiabilité, et l'exploitabilité 17
5 Leadership 18
5.4 Rôles, responsabilités et autorités sur les processus de dématérialisation ou de conservation 18
5.5 Leadership et engagement de PSDC 19
6 Planification 20
6.1.4 Risques liés à l'activité PSDC 20
7 Support 21
7.4 Sensibilisation à la politique de dématérialisation ou de conservation 21
7.5.4 La non-répudiation des informations documentées 21
8 Fonctionnement 21
8.4 Acceptation des risques 21
9 Évaluation des performances 21
9.1 Surveillance, mesures, analyse et évaluation 21
9.2 Audit interne 22
9.3 Revue de direction 22
10 Amélioration 22
10.2 Amélioration continue 22
**5 Code de bonnes pratiques spécifiques aux PSDC en relation avec ISO/IEC 27002:2013** 23
5 Politiques de sécurité de l'information 23
5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation 23
5.2.1 Politiques de dématérialisation ou de conservation 23
5.2.2 Revue de la politique de dématérialisation ou de conservation 24
6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation 24
6.1 Organisation interne 24
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation 24
6.1.2 Séparation des tâches 25
6.1.5 La sécurité de l'information dans la gestion de projet 26
6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation 26
6.3.1 Vérification des documents numériques après dématérialisation 26
6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques 26
6.3.3 Gestion des preuves 26
6.3.4 Relations avec l'autorité nationale 27

6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients 27
6.4.1 La sécurité dans les accords avec le client 27
6.4.2 Obligation d'information préalable du client 28
6.4.3 Classification des actifs du client 29
6.4.4 Obligation d'information du client en cas de changements ou d'incidents 29
7 La sécurité des ressources humaines 30
7.2 Pendant la durée du contrat 30
7.2.4 Engagement envers les politiques 30
8. Gestion des actifs 31
8.1 Responsabilités relatives aux actifs 31
8.1.1 Inventaire des actifs 31
8.1.2 Propriété des actifs 31
8.1.4. Cloisonnement d'informations secrètes ou d'informations à caractère personnel 31
8.2 Classification de l'information 32
8.2.1 Classification des informations 32
8.3 Manipulation des supports 32
8.3.2 Mise au rebut des supports 32
9 Contrôle d'accès 33
9.1 Exigences métier en matière de contrôle d'accès 33
9.1.3 Ségrégation effective liée aux droits d'accès 33
10 Cryptographie 33
10.1 Mesures cryptographiques 33
10.1.1 Politique d'utilisation des mesures cryptographiques 33
10.1.3 Authentification à deux facteurs 33
10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques 34
10.1.5 Protection de l'intégrité des documents internes 34
10.1.6 Signature électronique des documents internes 35
10.1.7 Protection des transmissions de documents 35
10.1.8 Conservation des signatures électroniques 36
11 Sécurité physique et environnementale 36
11.1 Zones sécurisées 36
11.1.7 Accompagnement des visiteurs 36
11.2 Matériels 37
11.2.1 Emplacement et protection du matériel 37
11.2.5 Sortie des actifs 37
12 Sécurité liée à l'exploitation 37
12.1 Procédures et responsabilités liées à l'exploitation 37

12.1.5 Procédures d'exploitation du SDC 37
12.4 Journalisation et surveillance 38
12.4.1 Journalisation des événements 38
12.4.3 Journaux administrateur et opérateur 38
12.4.4 Synchronisation des horloges 39
12.4.5 Exploitabilité des journaux d'événements 39
12.8 Gestion correcte et sécurisée du SDC 39
12.8.1 Adéquation du SDC 39
12.8.2 Description détaillée du SDC 40
12.8.3 Mécanismes de sécurité du SDC 40
12.8.4 Supervision des aspects opérationnels du SDC 41
12.8.5 Contrôle régulier de l'intégrité du SDC 41
13 Sécurité des communications 42
14 Acquisition, développement et maintenance des systèmes d'information 42
14.1 Exigences de sécurité applicables aux systèmes d'information 42
14.1.1 Analyse et spécification des exigences de sécurité de l'information 42
15. Relations avec les fournisseurs 43
15.1 Sécurité de l'information dans les relations avec les fournisseurs 43
15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation. 43
16 Gestion des incidents liés à la sécurité de l'information 44
16.1 Gestion des incidents liés à la sécurité de l'information et améliorations 44
16.1.1 Responsabilités et procédures 44
17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 44
17.3 Continuité de l'activité et du SDC 44
17.3.1 Organisation de la continuité 44
17.3.2 Mise en œuvre de la continuité 45
17.3.3 Vérifier, revoir et évaluer la continuité 45
18 Conformité 45
18.1 Conformité aux obligations légales et réglementaires 45
18.1.3 Protection des enregistrements 45
18.2 Revue de la sécurité de l'information 46
18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation 46
18.2.5 Revue indépendante de la sécurité du SDC 47

**Annexe A (normative) : Objectifs et mesures de référence spécifiques aux PSDC** 48
5 Politiques de sécurité de l'information 48
5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation 48
5.2.1 Politiques de dématérialisation ou de conservation 48
5.2.2 Revue de la politique de dématérialisation ou de conservation 48
6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation 49
6.1 Organisation interne 49
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation 49
6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation 49
6.3.1 Vérification des documents numériques avant destruction des documents analogiques correspondants 49
6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques 49
6.3.3 Gestion des preuves 49
6.3.4 Relations avec l'autorité nationale 49
6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients 50
6.4.1 La sécurité dans les accords avec les clients 50
6.4.2 Obligation d'information préalable du client 50
6.4.3 Classification des actifs du client 50
6.4.4 Obligation d'information du client en cas de changements ou d'incidents 50
7 La sécurité des ressources humaines 50
7.2 Pendant la durée du contrat 50
7.2.4 Engagement envers les politiques 50
8. Gestion des actifs 50
8.1 Responsabilités relatives aux actifs 50
8.1.4 Cloisonnement d'informations secrètes ou d'informations à caractère personnel 50
9 Contrôle d'accès 51
9.1 Exigences métier en matière de contrôle d'accès 51
9.1.3 Ségrégation effective liée aux droits d'accès 51
10 Cryptographie 51
10.1.3 Mesures d'authentification à deux facteurs 51
10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques 51
10.1.5 Protection de l'intégrité des documents internes 51
10.1.6 Signature électronique des documents internes 51
10.1.7 Protection des transmissions de documents 51
10.1.8 Conservation des signatures électroniques 51
11 Sécurité physique et environnementale 52

11.1 Zones sécurisées 52
11.1.7 Accompagnement des visiteurs 52
12 Sécurité liée à l'exploitation 52
12.1 Procédures et responsabilités liées à l'exploitation 52
12.1.5 Procédures d'exploitation du SDC 52
12.4.5 Exploitabilité des journaux d'événements 52
12.8 Gestion correcte et sécurisée du SDC 52
12.8.1 Adéquation du SDC 52
12.8.2 Description détaillée du SDC 52
12.8.3 Mécanismes de sécurité du SDC 52
12.8.4 Supervision des aspects opérationnels du SDC 53
12.8.5 Contrôle régulier de l'intégrité du SDC 53
15. Relations avec les fournisseurs 53
15.1 Sécurité de l'information dans les relations avec les fournisseurs 53
15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation 53
17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité 53
17.3 Continuité de l'activité et du SDC 53
17.3.1 Organisation de la continuité 53
17.3.2 Mise en œuvre de la continuité 53
17.3.3 Vérifier, revoir et évaluer la continuité 53
18 Conformité 53
18.2 Revue de la sécurité de l'information 53
18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation 53
18.2.5 Revue indépendante de la sécurité du SDC 54

# 0 Introduction

## 0.1 Contexte

La présente règle technique (ci-après « la Règle technique ») définit des exigences et des mesures permettant à une organisation d'établir une gestion de la sécurité de l'information et une gestion opérationnelle spécifiques aux processus de dématérialisation ou de conservation.

Du point de vue de la gestion de la sécurité de l'information, la Règle technique se base sur les Normes internationales ISO/IEC 27001:2013 et ISO/IEC 27002:2013 de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer :

a) un Système de Management de la Sécurité de l'Information (ci-après « SMSI ») basé sur la Norme internationale ISO/IEC 27001:2013 et intégrant les processus de dématérialisation ou de conservation,
b) des objectifs et des mesures de la sécurité de l'information basés sur la Norme internationale ISO/IEC 27002:2013 et spécifiques aux processus de dématérialisation ou de conservation.

La Règle technique a été rédigée selon des exigences de la norme ISO/IEC 27009:2016.

La Règle technique est aussi utilisée pour les audits d'évaluation de la conformité d'une organisation exécutant des processus de dématérialisation ou de conservation.

Ces audits d'évaluation ne doivent pas uniquement porter sur les exigences et les mesures de sécurité, mais aussi sur les préconisations de mise en œuvre. Toute déviation par rapport à ces préconisations, qui n'est pas dûment argumentée, documentée ou évidente, peut donner lieu à une non-conformité mineure. Toute déviation par rapport aux mesures, sauf si l'exclusion de la mesure est dûment justifiée par le processus de traitement des risques ainsi que toute déviation par rapport aux exigences, doit donner lieu à une non-conformité mineure ou majeure telle que définie dans ISO/IEC 17021-1:2015.

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ci-après ILNAS) est la seule autorité nationale luxembourgeoise habilitée à conférer à une organisation un statut de prestataire de services de dématérialisation ou de conservation (ci-après statut de PSDC), si cette organisation a été certifiée conforme à la Règle technique par un organisme de certification accrédité pour cette activité selon les exigences de la Norme internationale ISO/IEC 17021-1:2015, « Évaluation de la conformité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management » ainsi que les exigences complémentaires de la Norme ISO/IEC 27006:2015 « Requirements for bodies providing audit and certification of information security management systems ». Ces normes définissent les exigences pour réaliser des certifications à reconnaissance internationale de systèmes de management selon la norme ISO/IEC 27001:2013 et la Règle technique.

La Règle technique ne se substitue pas aux règlements, lois, ou normes applicables aux organisations exécutant des processus de dématérialisation ou de conservation. En particulier, le règlement (UE) n °910/2014 du Parlement Européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (aussi appelé règlement « eIDAS ») doit être considéré comme une fondation pour l'établissement des propriétés de sécurité qui y sont exposées, notamment en matière de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

## 0.2 Structure du document

Ce document est structuré de la façon suivante :

- Le chapitre 1 précise le domaine d'application de la Règle technique.
- Le chapitre 2 cite des références normatives, c'est-à-dire les normes à respecter par les organisations mettant en application la Règle technique.
- Le chapitre 3 définit les termes utilisés dans ce texte.

- Le chapitre 4 cite des exigences spécifiques pour le système de management des prestataires de service de dématérialisation ou de conservation. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27001:2013 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences », d'où la numérotation non linéaire des exigences : un complément à une section existante de la norme initiale garde le même numéro, les sections non modifiées ne sont pas incluses dans le présent document, et les nouvelles sections prennent des numéros qui ne sont pas utilisés dans la norme ISO/IEC 27001:2013.
- Le chapitre 5 définit des guidances spécifiques, en particulier des objectifs, des mesures de sécurité, des préconisations de mise en œuvre et des informations complémentaires. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27002:2013 « Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information », d'où la numérotation non linéaire des exigences.
- L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés au Chapitre 5 tout en rendant leur examen obligatoire dans le traitement des risques.

Les transitions requises par ISO/IEC 27009:2016 sont indiquées en *italique*.

# 1 Domaine d'application

La loi du 25 juillet 2015 relative à l'archivage électronique dispose qu'une personne peut, si elle détient une certification selon les exigences et les mesures définies dans la Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (ci-après PSDC), en regard de l'exécution de ses processus de dématérialisation ou de conservation, procéder à une notification auprès de l'ILNAS, en vue d'obtenir le statut de PSDC.

Si les critères de vérification établis par la loi relative à l'archivage électronique et par le système de qualité ad hoc du Département de la confiance numérique de l'ILNAS sont validés, l'ILNAS procèdera à l'inscription de la personne concernée dans la liste des PSDC, précisant les processus relatifs à la certification, établissant ainsi le statut de PSDC. Tout événement ou incident significatif détecté et tout changement majeur relatif à la portée de la certification, doit obligatoirement être notifié à l'ILNAS. Tout retrait, suspension ou non-renouvellement de la certification entraîne de facto le retrait du statut de PSDC.

Le statut de PSDC demeure volontaire, sauf disposition réglementaire ou sectorielle l'imposant.

La certification effective selon la Règle technique d'exigences et de mesures pour la certification des PSDC de toute personne permet la demande du statut de prestataire de services de dématérialisation ou de conservation délivré par le Département de la confiance numérique de l'ILNAS. L'ILNAS reconnaît formellement, via ce statut, la personne concernée en tant que PSDC.

La personne certifiée doit être en mesure de garantir les résultats de l'exécution des processus de dématérialisation ou de conservation pour lesquels elle a obtenu la certification. La certification garantit que les documents numériques résultants de la numérisation des documents analogiques et les archives numériques seront reconnus comme conformes aux exigences spécifiques liées à l'activité de dématérialisation respectivement de conservation, telles qu'établies dans ce document.

Ainsi une copie sera présumée être conforme à l'original si elle est produite par le processus ad hoc d'un PSDC. De même, une archive numérique est considérée comme équivalente aux originaux numériques, si elle est conservée par le processus ad hoc d'un PSDC.

Indépendamment de son type, de sa taille, de ses processus ou de ses activités, pour ses besoins internes ou dans le cadre de services proposés à ses clients, la Règle technique d'exigences et de mesures des PSDC est applicable à toute organisation publique ou privée.

La Règle technique a été définie à partir de Normes internationales publiées et maintenues par l'Organisation Internationale de Normalisation (ci-après « ISO »).

La Règle technique doit donc être considérée comme un supplément à ces normes[(1)] en amendant et complétant leur contenu spécifiquement aux processus de dématérialisation ou de conservation.

# 2 Références normatives

Les documents de référence suivants sont indispensables pour l'application de la Règle technique.

Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

*ISO/IEC 27000:2016, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire*

*ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information -- Exigences*

*ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*

# 3 Termes et définitions

Pour les besoins de la Règle technique, les abréviations suivantes s'appliquent :

| | |
|---|---|
| DdA | Déclaration d'Applicabilité (terme anglais : Statement of Applicability (SoA), déclaration relative à l'applicabilité des objectifs et mesures de sécurité) |
| eIDAS | Règlement (UE) No 910/2014 du Parlement Européen de du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE |
| L2TP | Layer 2 Tunneling Protocol (terme anglais) |
| IPSec | Internet Protocol Security (terme anglais) |
| PPP | Point to Point Protocol (terme anglais) |
| PSDC | Prestataire de Services de Dématérialisation ou de Conservation |
| SDC | Système de Dématérialisation ou de Conservation |
| SFTP | SSH File Transfer Protocol (terme anglais) |
| SMSI | Système de Management de la Sécurité de l'Information |
| SSH | Secure SHell (terme anglais) |
| TLS | Transport Layer Security (terme anglais) |
| UTC | Temps Univers |

Pour les besoins de la Règle technique, les termes et définitions fournis dans la norme ISO/IEC 27000:2016 ainsi que les définitions supplémentaires suivantes s'appliquent.

## 3.1 actif

tout élément représentant de la valeur pour l'organisation

Note 1 : Il existe plusieurs sortes d'actifs, dont :

a) l'information,
b) les documents,
c) les archives,
d) les actifs techniques, par exemple un scanneur, un serveur ou des disques durs,
e) les actifs techniques immatériels, par exemple des unités de stockage virtuelles,
f) le personnel d'une organisation,
g) les actifs incorporels, par exemple la réputation et l'image,
h) les processus et services.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.2.

## 3.2 analogique

non numérique

Note : Un support de stockage analogique est un support de stockage non numérique, par exemple le papier, le film argentique ou le disque vinyle.

## 3.3 archive

document conservé en l'état en vue d'une utilisation pérenne

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.1.

## 3.4 archive numérique

archive sous forme de document numérique

## 3.5 authenticité

propriété selon laquelle une entité est ce qu'elle revendique être

[ISO/IEC 27000:2016]

## 3.6 confidentialité

propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés

[ISO/IEC 27000:2016]

## 3.7 conservation (électronique)

l'activité qui consiste à conserver un original numérique ou une copie à valeur probante dans des conditions qui assurent des garanties fiables quant au maintien de l'intégrité du document conservé

[loi du 25 juillet 2015, art. 2 b]

Note : Dans la suite du document, le terme « conservation » est synonyme de « conservation électronique », sauf précision contraire

## 3.8 dématérialisation

l'activité qui consiste à créer une copie à valeur probante d'un original existant sous forme analogique dans des conditions qui assurent des garanties fiables quant à la conformité de la copie ainsi créée à l'original

[loi du 25 juillet 2015, art. 2 d]

## 3.9 disponibilité

propriété d'être accessible et utilisable à la demande par une entité autorisée

[ISO/IEC 27000:2016]

## 3.10 document

information ou objet documentaire enregistré qui peut être traité comme une unité

[ISO 15489 -1:2001]

## 3.11 fiabilité

propriété relative à un comportement et des résultats prévus et cohérents

[ISO/IEC 27000:2016]

## 3.12 gestion

définition, mise en œuvre ou en exploitation, opération, contrôle, révision, maintenance et amélioration

Note : De même, gérer est synonyme de « définir, mettre en œuvre ou en exploitation, opérer, contrôler, réviser, maintenir et améliorer ».

## 3.13 indexation

définition de points d'accès pour faciliter la recherche des documents

Note 1 : La génération de métadonnées liées aux documents numériques et aux archives numériques est généralement utilisée pour faciliter leur recherche.

Note 2 : Définition adaptée de la norme ISO 15489 -1:2001, définition 3.11.

## 3.14 intégrité

propriété d'exactitude et de complétude

[ISO/IEC 27000:2016]

## 3.15 métadonnées

données décrivant le contexte, le contenu ou la structure des documents ainsi que leur gestion dans le temps

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.6.

## 3.16 non-répudiation

capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine

[ISO/IEC 27000:2016]

## 3.17 organisme

personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs

Note 1 : Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

[ISO/IEC 27000:2016]

Note 2 : Le terme organisme désigne le prestataire qui est ou qui veut être prestataire de service de dématérialisation ou de conservation.

## 3.18 prestataire de services de dématérialisation ou de conservation (PSDC)

toute personne qui exerce à titre principal ou accessoire, pour ses propres besoins ou pour compte d'autrui, des activités de dématérialisation ou de conservation électronique et qui est, dans les conditions et selon les modalités de la [loi 25 juillet 2015], certifiée à cette fin et inscrite sur la liste visée à l'article 4 (3) [de cette loi]

[loi du 25 juillet 2015, art. 2h]

Note : Les prestataires ne sont concernés que par les processus qu'ils gèrent. Dans tout ce document, le « ou » peut être inclusif ou exclusif selon le contexte opérationnel du prestataire.

## 3.19 preuve

document démontrant l'effectivité d'une opération

Note 1 : La preuve d'une opération signifie qu'il peut être démontré qu'elle a été créée dans le cadre normal de la conduite de l'activité de l'organisation et qu'elle est intacte et complète. Ne se limite pas au sens légal du terme.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.5.

## 3.20 processus

ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[ISO 9000:2015]

## 3.21 sécurité de l'information

protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

Note : En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

[ISO/IEC 27000:2016]

Note pour les PSDC : les propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, la fiabilité et l'exploitabilité sont incluses dans la notion de sécurité.

## 3.22 système

ensemble d'actifs techniques corrélés ou interactifs

## 3.23 système de conservation

système composé d'un ensemble d'actifs techniques permettant le stockage temporaire des documents numériques en vue de leur conservation électronique, leur conversion en archives numériques, leur suppression et la conservation des archives numériques aussi longtemps que nécessaire, leur exploitation, leur restitution partielle ou totale, leur transfert et leur suppression

## 3.24 système de dématérialisation

système composé d'un ensemble d'actifs techniques permettant la création des documents numériques à partir des documents analogiques, le stockage temporaire des documents analogiques et numériques, leur restitution, leur transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques

## 3.25 système de dématérialisation ou de conservation (SDC)

système de dématérialisation, système de conservation, ou un système combinant les deux

# 4 Exigences spécifiques pour PSDC et complémentaires à la norme ISO/IEC 27001:2013

## 4.1 Structure de ce standard

*Ce standard est un standard lié à la norme ISO/IEC 27001:2013. Il est spécifique aux PSDC au sens de la loi du 25 juillet 2015 relative à l'archivage électronique.*

*Les objectifs de sécurité et les mesures de sécurité spécifiques sont indiqués dans l'Annexe A.*

## 4.2 Exigences spécifiques aux systèmes de management des PSDC

*Toutes les exigences des chapitres 4 à 10 de la norme ISO/IEC 27001:2013 qui ne figurent pas ci-dessous restent applicables sans modification.*

### 4 Contexte de l'organisation

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

### 4.0 Système de Management des processus de dématérialisation ou de conservation

L'organisation doit gérer un système de management des processus de dématérialisation ou de conservation, intégré au SMSI ou répondant aux mêmes exigences, pour assurer le déroulement adéquat des processus de dématérialisation ou de conservation, la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liés aux processus de dématérialisation ou de conservation.

Ce système de management des processus et le SMSI, ou le système de management intégrant ces deux aspects doit s'appliquer aux processus et activités liés à la prestation de services du PSDC et à tous les actifs supportant ces processus.

*L'exigence 4.3 de la norme ISO/IEC 27002:2013 est complétée de la façon suivante.*

### 4.3 Détermination du domaine d'applicabilité

Pour établir le domaine d'application du système de management des processus de dématérialisation ou de conservation, l'organisation doit en déterminer les limites et l'applicabilité.

Elle doit définir la nature des processus (dématérialisation ou conservation), le type des documents concernés et le type des clients (internes ou externes à l'organisation, secteurs concernés) qui peuvent bénéficier des services du PSDC.

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

### 4.5 L'authenticité, la fiabilité, et l'exploitabilité

En complément des propriétés de sécurité de base qui sont:

a. la confidentialité,
b. l'intégrité, et

c. la disponibilité,

le système de management doit gérer les propriétés de sécurité complémentaires suivantes :

d. l'authenticité (souvent considéré comme un volet particulier de l'intégrité) :
   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont authentiques, à savoir :
   i. Les documents analogiques ou numériques ont bien été transmis par la personne qui est supposée les avoir transmis.
   ii. Le document numérique résultant de la numérisation d'un document analogique ou l'archive numérique a bien été créé par la personne ou le système au moment présumé.
   iii. Le document numérique ou l'archive numérique est bien ce qu'il est supposé être.

e. la fiabilité :
   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont fiables, à savoir :
   i. Toutes les activités effectuées dans le cadre de l'établissement des processus de dématérialisation ou de conservation sont exécutées conformément aux politiques et aux procédures définies et mises en œuvre par l'organisation en la matière.
   ii. Le document numérique ou l'archive numérique créé et exploité est conforme à son état original et non modifié par des modifications non autorisées.

f. l'exploitabilité :
   L'organisation doit pouvoir démontrer que l'exploitation des processus de dématérialisation ou de conservation crée un document numérique ou une archive numérique qui soit à tout moment localisable, lisible, intelligible, utilisable avec les informations nécessaires à la compréhension de son origine et disponible aussi longtemps que nécessaire.

Note : C'est en ajoutant ces propriétés dans l'envergure du SMSI qu'on généralise le système de management de la norme ISO/IEC 27001:2013 limité à la sécurité de l'information, à un système de management de toutes les propriétés requises aux activités de dématérialisation ou de conservation.

# 5 Leadership

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 5.4 Rôles, responsabilités et autorités sur les processus de dématérialisation ou de conservation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par les processus de dématérialisation ou de conservation sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de :

a. s'assurer que le système de management des processus de dématérialisation ou de conservation est conforme aux exigences du présent document ;
b. définir les critères de performances ;
c. rendre compte à la direction des performances du système de management des processus de dématérialisation ou de conservation ;
d. gérer la documentation (politiques, procédures) supportant ces processus ;
e. définir le système, son fonctionnement et sa sécurité au niveau opérationnel ;
f. superviser la mise en œuvre de la politique ;
g. émettre des recommandations en vue d'améliorer la gestion opérationnelle ;
h. définir et approuver les méthodes relatives à la gestion des risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires ;

i. gérer les risques pouvant impacter la stabilité financière de l'organisation et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;
j. évaluer l'adéquation des mesures adoptées en vue de mitiger les risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation, et jugées non acceptables par la direction de l'organisation ;
k. évaluer l'opportunité d'une couverture d'assurance pour garantir la continuité de l'exécution des processus de dématérialisation ou de conservation de l'organisation même en cas de cessation d'activité et pendant une période minimum de transition ;
l. identifier les changements en termes de risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;
m. sensibiliser le personnel (de l'organisation et des tiers) concerné quant aux risques ;
n. identifier et évaluer les problèmes et les incidents ;
o. émettre des recommandations quant aux actions préventives et correctives à adopter en réponse aux problèmes et aux incidents évalués.

La direction doit attribuer chaque rôle et responsabilité à une personne ou à une entité dont les membres et le mode de fonctionnement sont documentés, et réviser régulièrement cette attribution.

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 5.5 Leadership et engagement de PSDC

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management en :

a. s'assurant qu'une politique et des objectifs sont établis en matière de processus de dématérialisation ou de conservation et qu'ils sont compatibles avec l'orientation stratégique de l'organisation dûment documentée et avec la politique de sécurité de l'information ;
   Note : Une politique dédiée aux processus de dématérialisation et une politique dédiée au processus de conservation peuvent être établies par l'organisation. Si un des processus n'est pas dans le domaine d'applicabilité, cette politique et toutes les exigences y relatives ne sont évidemment pas requises.
b. s'assurant que les exigences de cette politique sont intégrées aux processus ;
c. s'assurant que les ressources nécessaires pour le système de management des processus de dématérialisation ou de conservation sont disponibles (en particulier pour fournir les éléments probants quant à l'intégrité et la fiabilité) ;
d. communiquant sur l'importance de disposer d'un management des processus de dématérialisation ou de conservation efficace et de se conformer à ses exigences ;
e. s'assurant que le système de management des processus de dématérialisation ou de conservation produit le ou les résultats escomptés ;
f. orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du processus de dématérialisation ou de conservation ;
g. promouvant l'amélioration continue ;
h. aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités ;
i. fournissant la preuve de l'existence légale de l'organisation ;
j. fournissant la preuve d'une situation financière suffisante et d'une situation stable pour répondre aux attentes des parties intéressées à l'activité de PSDC ;
   Note : L'organisation peut mener une étude sur le coût d'un transfert d'activités ou d'une restitution à tous les clients des documents y inclus toutes les informations requises pour maintenir la valeur probante d'un document dématérialisé et d'une archive numérique. L'étude pourra montrer que ce coût est inférieur aux provisions, aux réserves, ou au capital disponible de l'organisation, et que ces

paramètres sont stables. L'organisation peut mettre en place un processus de monitoring de ces paramètres qui assure une gestion d'incident en cas de dégradation de la stabilité financière.

Note : Une organisation de droit privé pourra par exemple fournir les informations suivantes :

- □ une étude sur le coût d'un transfert d'activités et la justification de pouvoir le réaliser à tout moment, compte tenu de son capital, de ses réserves, ou de ses provisions,
- □ les bilans et comptes de résultat des 3 dernières années fiscales, pour autant que l'ancienneté de l'organisation le permette,
- □ rapport ou avis financier émis par une autorité de surveillance luxembourgeoise,
- □ niveau d'exposition des activités métiers aux facteurs externes à l'organisation,
- □ rapport d'auditeurs financiers.

k. fournissant la garantie de continuité d'exécution (c'est-à-dire, pendant une période de transition minimum permettant d'assurer un transfert) des processus de dématérialisation ou de conservation, en particulier pour les cas suivants :
   1. processus de dématérialisation exécuté par l'organisation pour le compte d'un tiers,
   2. processus de conservation électronique exécuté par l'organisation pour le compte d'un tiers,
   3. sous-processus de restitution, transfert et suppression des archives numériques exécuté par l'organisation pour son propre compte.

   Cette garantie de continuité doit être gérée par l'organisation et couvrir le risque économique de cessation d'activités.

   Note : Un moyen pour l'organisation de garantir cette continuité d'exécution pendant une période de transition minimum est par exemple de contracter une assurance spécifique ou d'obtenir un engagement formel d'un actionnaire institutionnel ou privé majoritaire se portant garant.

# 6 Planification

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 6.1.4 Risques liés à l'activité PSDC

L'organisation doit:

a. intégrer les risques de sécurité de l'information et opérationnels associés à la gestion des processus de dématérialisation ou de conservation dans son processus d'identification (6.1.2 c) d'analyse (6.1.2.d) et d'évaluation des risques (6.1.2.e), y intégrer également les risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à ces processus ;
b. appliquer son processus de traitement des risques de sécurité aux risques déterminés au point précédent ;
c. comparer les objectifs et les mesures déterminés en 6.1.3 b) avec celles de l'Annexe A du présent document et vérifier qu'aucune mesure nécessaire n'a été omise ;
d. compléter la déclaration d'applicabilité déterminée en 6.1.3 d) avec les mesures de l'Annexe A de la Règle technique et la justification de leur insertion ou de leur exclusion, ainsi que, le cas échéant, l'indication de leur mise en œuvre ;
e. porter à connaissance des clients et à l'ILNAS la déclaration d'applicabilité, notamment si elle contient des exclusions.

Une exclusion doit être rejetée si elle crée une non-conformité avec une exigence légale, réglementaire ou contractuelle.

# 7 Support

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 7.4 Sensibilisation à la politique de dématérialisation ou de conservation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent :

1. être sensibilisées à la politique de dématérialisation ou de conservation et respecter toute la documentation relative à cette politique ;
2. avoir conscience de leur contribution à l'efficacité du système de management, y compris aux effets positifs d'une amélioration des performances ;
3. avoir conscience des implications de toute non-conformité aux exigences requises par le système de management ;
4. connaitre leurs responsabilités en vertu de la loi luxembourgeoise en matière de dématérialisation ou de conservation et concernant les processus de dématérialisation ou de conservation.

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 7.5.4 La non-répudiation des informations documentées

L'organisation doit mettre en place un environnement documentaire permettant de démontrer envers un tiers le respect des propriétés de sécurité indiquées au chapitre 4.5 du présent document et l'intégrité de la documentation.

# 8 Fonctionnement

*Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :*

## 8.4 Acceptation des risques

L'organisation doit faire accepter par la direction l'appréciation des risques, le plan de traitement des risques incluant une indication des ressources requises, le niveau du risque actuel et celui après traitement.

L'organisation doit conserver la preuve de cette acceptation et la documentation de la délibération par la direction.

# 9 Évaluation des performances

*L'exigence 9.1 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.*

## 9.1 Surveillance, mesures, analyse et évaluation

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit évaluer les performances de son SDC, ainsi que l'efficacité du système de management des processus de dématérialisation et de conservation.

*L'exigence 9.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.*

## 9.2 Audit interne

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management des processus de dématérialisation et de conservation

a. est conforme :
    1. aux exigences propres de l'organisation concernant son système de management de processus de dématérialisation ou de conservation
    2. à cette règle technique ;
b. est efficacement mis en œuvre et tenu à jour.

L'organisation doit donc inclure ces audits dans le ou les programmes d'audit, définir les critères d'audit et le périmètre de chaque audit, sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit, s'assurer qu'il est rendu compte des résultats des audits à la direction concernée, et conserver des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

*L'exigence 9.3 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.*

## 9.3 Revue de direction

De la même façon que pour le système de management de la sécurité de l'information, la direction doit procéder à la revue du système de management des processus de dématérialisation ou de conservation mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de direction doit prendre en compte :

g. les résultats de l'analyse de risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation de manière régulière.

La revue de direction doit avoir lieu au moins une fois par an et suite à des changements significatifs :

1. impactant le fonctionnement de l'organisation,
2. issus des besoins actuels de l'organisation,
3. de nature légale et réglementaire ayant un impact sur les activités et les processus de l'organisation.

# 10 Amélioration

*L'exigence 10.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.*

## 10.2 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management des processus de dématérialisation ou de conservation.

# 5 Code de bonnes pratiques spécifiques aux PSDC en relation avec ISO/IEC 27002:2013

*Toutes les catégories de mesures, objectifs de sécurité, mesures, préconisations de mise en œuvre, et informations supplémentaires de la norme ISO/IEC 27002:2013 qui ne figurent pas ci-dessous restent applicables sans modification.*

*L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés dans ce chapitre tout en les rendant leur examen obligatoire dans le traitement des risques.*

## 5 Politiques de sécurité de l'information

*Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :*

## 5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation

Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

### 5.2.1 Politiques de dématérialisation ou de conservation

#### Mesure

Il convient de définir une « politique de dématérialisation ou de conservation », de la faire approuver par la direction, de la mettre en application, de la diffuser et de la communiquer aux salariés et aux tiers concernés.

#### Préconisations de mise en œuvre

Il convient que la politique de dématérialisation ou de conservation définisse le domaine d'application des processus de dématérialisation ou de conservation, la gestion de la sécurité de l'information et la gestion opérationnelle appliqués à ce processus.

Il convient que ce document contienne les éléments suivants :

a. une présentation de l'organisation, de son historique et de ses activités métiers ;
b. le lien avec la stratégie ou la motivation d'implémenter cette activité ;
c. une définition du domaine d'application des processus de dématérialisation ou de conservation ;
d. une description générale organisationnelle et technique des processus suivants sous-jacents
    1. au processus de dématérialisation :
        i. collecte des documents analogiques,
        ii. création et stockage temporaire des documents numériques,
        iii. stockage temporaire des documents analogiques,
        iv. restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques,
        v. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;
    2. au processus de conservation :
        i. collecte des documents numériques,
        ii. création et conservation des archives numériques,
        iii. restitution, transfert, suppression des archives numériques,

iv. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;

e. une description générale technique du SDC et de son niveau de conformité à des normes et des référentiels reconnus ;
f. les rôles et les responsabilités spécifiques au processus de dématérialisation ou de conservation et aux processus sous-jacents exécutés par l'organisation et en matière de gestion de la sécurité de l'information et de gestion opérationnelle ;
g. les grands principes de sécurité de l'information appliqués au processus de dématérialisation ou de conservation exécuté par l'organisation, notamment en matière d'authenticité, de fiabilité et d'exploitabilité ;
h. les références aux lois et aux règlements applicables à l'organisation et spécifiques au processus de dématérialisation ou de conservation ;
i. la gestion de la documentation supportant le processus de dématérialisation ou de conservation ;
j. des références aux documents, comme les procédures d'administration, d'opérations et de sécurité, supportant la politique de dématérialisation ou de conservation ;
k. les modalités de revue de la politique de dématérialisation ou de conservation.

### 5.2.2 Revue de la politique de dématérialisation ou de conservation

#### Mesure

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité de la politique de dématérialisation ou de conservation, il convient de revoir ces politiques et les processus y relatifs à intervalles programmés et en cas de changements majeurs.

#### Préconisations de mise en œuvre

Les mêmes préconisations que pour la politique de sécurité de l'information s'appliquent à cette politique.

*La catégorie « 6 Organisation de la sécurité de l'information » est complétée de la façon suivante.*

## 6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation

## 6.1 Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.

### 6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation

#### Mesure

Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables.

### Préconisations de mise en œuvre

Il convient d'attribuer les responsabilités conformément à la politique de sécurité de l'information (voir 5.1.1 de l'ISO/IEC 27002:2013) et à la politique de dématérialisation ou de conservation (voir 5.2.1 du présent document).

Il convient de déterminer les responsabilités relatives à la protection des actifs et la mise en œuvre de processus de sécurité spécifiques et des processus de dématérialisation ou de conservation.

Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et d'exploitation des processus de dématérialisation ou de conservation et en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information.

Il convient de préciser les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes :

a. il convient d'identifier et de déterminer les actifs et les processus de sécurité ainsi que les processus de dématérialisation ou de conservation ;
b. il convient d'affecter une personne ou une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail (voir 8.1.2) ;
c. il convient de définir et de documenter les différents niveaux d'autorisation ;
d. pour être à même d'assurer les responsabilités, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de facilités pour se tenir au courant des évolutions ;
e. Il convient d'identifier et de documenter les activités de coordination et de supervision liées aux relations avec les fournisseurs.

Il convient de désigner pour chaque processus de dématérialisation ou de conservation une personne pour chacune des responsabilités suivantes :

a. la gestion de la documentation (politiques, procédures) supportant ces processus,
b. leur définition au niveau opérationnel, incluant le SDC et les mécanismes de sécurité associés,
c. la supervision de leur mise en œuvre,
d. la définition de leurs critères de performances,
e. leur évaluation selon les critères de performances,
f. l'émission de recommandations en vue d'améliorer leur gestion opérationnelle.

### Informations supplémentaires

Les personnes auxquelles ont été attribuées des responsabilités peuvent déléguer des tâches. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée.

## 6.1.2 Séparation des tâches

### Préconisations de mise en œuvre

Il convient de s'assurer que les personnes assumant des rôles et des responsabilités dans la gestion de processus ou d'activités de la sécurité de l'information ou opérationnels liés à la dématérialisation ou la conservation, n'assument pas également la revue de l'efficacité de l'exécution de ces rôles et responsabilités ainsi que l'évaluation de leur conformité à des objectifs définis.

Il convient d'assurer une séparation effective des activités d'administration, d'opérations et de sécurité non seulement dans la description des rôles, mais aussi dans l'attribution des privilèges pour les comptes des utilisateurs autorisés à accéder au SDC, de manière à réduire les risques de conflits d'intérêts et d'accès non autorisés.

Pour respecter le principe de non-répudiation, il convient de pouvoir démontrer que les privilèges d'accès établis pour l'ensemble des utilisateurs du SDC, y compris les accès à travers des comptes techniques, respectent le principe de séparation effective des activités d'administration, d'opérations et de sécurité du système de conservation.

### 6.1.5 La sécurité de l'information dans la gestion de projet

#### Préconisations de mise en œuvre

Il convient de rédiger et d'approuver les procédures de gestion du SDC dans la définition et la mise en œuvre des projets de dématérialisation ou de conservation.

*Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :*

## 6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation

Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.

### 6.3.1 Vérification des documents numériques après dématérialisation

#### Mesure

Il convient d'exercer une vérification du contenu des documents numériques par rapport aux documents analogiques correspondants.

#### Préconisations de mise en œuvre

En ce qui concerne le processus de dématérialisation, il convient d'implémenter des

a. mécanismes de vérification de l'adéquation du nombre de documents analogiques en entrée (ou du nombre de pages composant ces documents) avec le nombre de documents (ou de pages) en sortie (numériques et analogiques rejetés), et des
b. mécanismes de vérification du contenu des documents numériques résultant de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

### 6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques

#### Mesure

Il convient de s'assurer que toute modification ou suppression des archives numériques créées, qui n'étaient pas programmées lors de la définition du projet de conservation, nécessitent l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

### 6.3.3 Gestion des preuves

#### Mesure

Il convient d'établir une procédure et de mettre en œuvre une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné.

### Préconisations de mise en œuvre

Il convient de s'assurer que l'intégrité du fonctionnement du SDC, des documents numériques et des archives numériques gérées par le SDC est vérifiée de manière régulière et suite à une modification significative du SDC et du processus de conservation.

## 6.3.4 Relations avec l'autorité nationale

### Mesure

Il convient de mettre en application des procédures pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence potentiellement importante sur le service de dématérialisation ou de conservation.

### Préconisations de mise en œuvre

Il convient notamment de considérer comme changements significatifs :

a. un changement de direction de l'organisation,
b. une modification du SDC impactant les processus associés,
c. une modification du périmètre d'activités gérées par des fournisseurs impactant les processus de dématérialisation ou de conservation exécutés par l'organisation.

*Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :*

# 6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients

Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.

## 6.4.1 La sécurité dans les accords avec le client

### Mesure

Il convient d'établir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.

### Préconisations de mise en œuvre

Si le client est interne à l'organisation ou appartient à la même entité juridique, le document contractuel peut être remplacé par un document interne établi et validé selon les pratiques de gestion documentaire de l'organisation.

Il convient d'établir avec le client les éléments suivants dans le cadre de la gestion d'un projet de dématérialisation ou de conservation :

a. le besoin en informations du client liées aux processus de dématérialisation ou de conservation ;
b. la description détaillée du projet de dématérialisation ou de conservation, en prenant en compte les aspects techniques, opérationnels, sécuritaires, légaux et réglementaires ;
c. la base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation pour sassurer l'authenticité, la fiabilité et l'exploitation des documents collectés (analogiques et numériques), des documents numériques et des archives numériques du client pendant l'exécution des processus de dématérialisation ou de conservation ;

d. les niveaux de service liés à l'exécution du SDC ;
e. la gestion des changements organisationnels et techniques pouvant impacter les processus de dématérialisation ou de conservation, ainsi que le SDC ;
f. la gestion des incidents (majeurs) impactant les processus de dématérialisation ou de conservation, ainsi que le SDC ;
g. le processus et les modalités à appliquer pour l'évaluation des services ainsi que l'acceptation des services par le client ;
h. les rôles et responsabilités du client et de l'organisation dans le cadre de la mise en œuvre du projet et les conséquences en cas de non-respect de ces rôles et de ces responsabilités ;
i. les points de contacts du client et de l'organisation, d'un point de vue contractuel, opérationnel et de la sécurité de l'information ;
j. l'implication du client dans l'appréciation et le traitement des risques.

La base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation peuvent être documentées dans la déclaration d'applicabilité (voir ISO/IEC 27001) ou dans un document appelé « exigences d'assurance de sécurité » selon les Critères Communs (voir ISO 15408).

Il convient que le client s'engage en particulier à fournir et maintenir une liste de personnes autorisées à :

a. soumettre et à récupérer des documents analogiques ;
b. accéder aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques ;
c. utiliser le SDC ;
d. demander la destruction et la suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

### Informations supplémentaires

Un changement d'un document contractuel nécessite l'accord des parties contractantes.

C'est à ce niveau que des mesures de sécurité particulières exigées par le client et complémentaires à celles que le PSDC établit de sa propre initiative peuvent être spécifiées.

## 6.4.2 Obligation d'information préalable du client

### Mesure

Préalablement à toute relation contractuelle avec un détenteur, il convient de mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.

### Préconisations de mise en œuvre

Il convient que le PSDC inclue dans les informations données à ses clients avant d'établir un contrat :

a. la procédure suivie pour la dématérialisation ou pour la conservation,
b. la procédure suivie afin de restituer les copies à valeur probante sous une forme lisible en garantissant la fidélité à l'original,
c. les modalités et conditions d'une éventuelle sous-traitance y compris le lieu de stockage des données,
d. les obligations légales que le PSDC doit observer,
e. les conditions contractuelles de réalisation des prestations, y compris les limites éventuelles de responsabilité du PSDC,
f. les normes et procédures mises en œuvre ainsi que les caractéristiques techniques essentielles des installations utilisées pour la réalisation des prestations,
g. les modalités d'information du client en cas de changement.

Il convient de convenir avec les clients (internes ou externes à l'organisation) qui sont impactés le déroulement détaillé et les règles à suivre dans le cadre de l'exécution et des processus de dématérialisation et de conservation.

Il convient d'inclure ce déroulement détaillé et ces règles dans les procédures d'exploitation des processus de dématérialisation et de conservation, et de les faire approuver par les clients concernés.

Il convient d'impliquer le client dans les changements des procédures qu'il a approuvées.

Il convient d'inclure dans ces procédures le déroulement détaillé :

a. de la collecte des documents analogiques (pour le processus de dématérialisation seulement),
b. de la collecte des documents numériques (pour la conservation),
c. du stockage temporaire des documents numériques,
d. de la création et la conservation des archives numériques (pour la conservation),
e. de la restitution, le transfert et la suppression des archives numériques (pour la conservation).

Il convient de notifier le client d'une suppression programmée d'une archive numérique du client si un calendrier de suppression spécifique à cette archive a été rédigé lors de la définition du projet de conservation.

En cas d'absence de calendrier de suppression pour une archive numérique, il convient de demander au préalable au client l'autorisation de la supprimer.

## 6.4.3 Classification des actifs du client

### Mesure

Il convient que le client définisse avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.

### Préconisations de mise en œuvre

Il convient que le client assume le rôle du propriétaire pour les informations qui lui appartiennent et qui sont gérées par l'organisation.

Il convient de sensibiliser le client au fait qu'il est responsable des exigences de classification définies et appliquées à ses documents (documents collectés, documents numériques ou archives numériques).

## 6.4.4 Obligation d'information du client en cas de changements ou d'incidents

### Mesure

Il convient d'informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

### Préconisations de mise en œuvre

Il convient d'informer dans les plus brefs délais le client :

a. en cas de survenance d'incidents pouvant impacter :
    1. les documents du client,
    2. les processus de dématérialisation ou de conservation utilisés par le client ou pour son compte,
    3. le SDC utilisé par le client ou pour son compte ;

b. en cas de tentatives d'accès aux documents du client gérés par l'organisation avec les identifiants de connexion du client et hors des conditions normales de leur utilisation, par exemple hors des heures normales de bureau.

Il convient de considérer comme changements significatifs les changements signalés à l'autorité nationale (voir 6.3.4).

Il convient d'appliquer une conversion d'une archive numérique dans un format différent de son format initial que sur confirmation écrite du client (interne à l'organisation et externe) concerné par cette archive.

Il convient d'informer le client sur l'effet du changement sur l'appréciation des risques.

Il convient de garder une preuve que cette information a eu lieu, et si le temps avant la mise en application est court, de demander l'approbation du client.

# 7 La sécurité des ressources humaines

## 7.2 Pendant la durée du contrat

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 7.2.4 Engagement envers les politiques

#### Mesure

Il convient que le personnel interne et celui des fournisseurs, s'ils sont impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, comprennent et s'engagent par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.

#### Préconisations de mise en œuvre

Il convient que le personnel interne et celui des fournisseurs impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation :

1. soient correctement informés de leurs rôles et responsabilités liés aux processus de dématérialisation ou de conservation ;
2. s'engagent par écrit à respecter les politiques de dématérialisation ou de conservation et la politique de sécurité de l'information ;
3. assistent à une formation initiale sous forme de sensibilisation pour présenter les politiques, les attentes et les besoins de l'organisation en la matière, afin de s'assurer d'une compréhension commune de ces éléments ;
4. assistent à une formation continue de manière à rappeler les exigences liées à la dématérialisation ou à la conservation et à présenter les procédures associées à ces exigences et les récentes modifications apportées à l'ensemble de la documentation liée aux domaines concernés.

# 8 Gestion des actifs

## 8.1 Responsabilités relatives aux actifs

*Des préconisations de mise en œuvre additionnelles sont :*

### 8.1.1 Inventaire des actifs

#### Préconisations de mise en œuvre

Il convient d'identifier :

a. les processus de dématérialisation ou de conservation,
b. les composants des systèmes de dématérialisation ou de conservation,
c. les clients,
d. les documents collectés (analogiques et numériques) des clients,
e. les documents numériques résultants de la numérisation des documents analogiques des clients,
f. les archives numériques des clients.

### 8.1.2 Propriété des actifs

#### Préconisations de mise en œuvre

Il convient que le propriétaire de chaque actif processus de dématérialisation ou de conservation :

d. approuve l'évaluation des aspects opérationnels du SDC au moins une fois par an et suite à une modification significative ;
e. revoie la description détaillée du SDC et les spécifications des mécanismes de sécurité du système de conservation de manière régulière (au moins une fois par an) et suite à une modification significative du SDC.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 8.1.4 Cloisonnement d'informations secrètes ou d'informations à caractère personnel

#### Mesure

Il convient de cloisonner d'éventuelles informations secrètes ou informations à caractère personnel de façon suffisante pour notamment pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.

#### Préconisations de mise en œuvre

En vue de respecter le règlement européen sur la protection des données à caractère personnel, en particulier le droit à l'oubli, il convient que le client ou le PSDC s'abstienne de mettre dans les métadonnées des informations à caractère personnel, si ces métadonnées font partie du système de traçabilité des opérations.

## 8.2 Classification de l'information

*Des préconisations de mise en œuvre additionnelles sont :*

### 8.2.1 Classification des informations

#### Préconisations de mise en œuvre

Il convient de définir des niveaux de classification et de les attribuer aux actifs inventoriés en intégrant les exigences relatives à l'authenticité, à la fiabilité et à l'exploitation aussi longtemps que nécessaire.

Il convient d'assurer une revue de ces lignes directrices en cas de changement des spécificités du SDC et en cas de changement des attentes des clients.

#### Informations supplémentaires

Un critère « fiabilité » peut être défini en complément d'autres critères. Il peut contenir plusieurs niveaux de précision d'une dématérialisation (couleur versus noir et blanc, encodage de la couleur, résolution) et attribuer un tel niveau spécifiquement aux documents collectés des clients et aux archives numériques des clients.

Le critère d'intégrité peut être utilisé pour inclure les exigences liées à l'authenticité.

Le critère de disponibilité peut être utilisé pour inclure les exigences liées à l'exploitabilité.

## 8.3 Manipulation des supports

*Des préconisations de mise en œuvre additionnelles sont :*

### 8.3.2 Mise au rebut des supports

#### Préconisations de mise en œuvre

Il convient d'envisager :

a. la destruction des éléments suivants, par des mécanismes sécurisés :
   1. les documents analogiques des clients selon les conditions définies dans les documents contractuels établis entre les clients et l'organisation,
   2. tout support de stockage de l'organisation contenant les informations des clients (incluant les documents et archives numériques) ou de nature confidentielle à l'organisation,
   3. la suppression de toutes les informations des clients, contenues dans les supports de stockage de l'organisation par des mécanismes sécurisés si ces supports ne peuvent pas être détruits de manière sécurisée ;
b. l'évaluation par un tiers pouvant attester l'effectivité de la destruction et de la suppression ;
c. en cas de recours à un fournisseur, la production d'une attestation de ce fournisseur stipulant que :
   1. les supports de stockage remis au tiers par l'organisation en vue de leur destruction sont bien ceux qui ont été détruits,
   2. les informations stockées dans les supports de stockage remis par l'organisation en vue de leur suppression ont bien été supprimées,
   3. la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports ont été respectivement effectuées par une méthode sécurisée basée sur les bonnes pratiques en la matière.

# 9 Contrôle d'accès

## 9.1 Exigences métier en matière de contrôle d'accès

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 9.1.3 Ségrégation effective liée aux droits d'accès

#### Mesure

Il convient d'impliquer trois personnes différentes dans la gestion d'un droit d'accès : une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.

#### Préconisations de mise en œuvre

Il convient qu'un administrateur de droits d'accès sur un SDC n'attribue ce droit que si le droit a été formellement autorisé selon la politique des droits d'accès pour une autre personne et que le respect des exigences de sécurité avec ce droit a été validé par une personne différente.

# 10 Cryptographie

## 10.1 Mesures cryptographiques

*Des préconisations de mise en œuvre additionnelles sont :*

### 10.1.1 Politique d'utilisation des mesures cryptographiques

#### Préconisations de mise en œuvre

Lors de l'élaboration d'une politique cryptographique, il convient de prendre en compte le point suivant :

h. l'application des services de confiance qualifiés conformes au règlement eIDAS pour assurer la sécurité des documents dématérialisés et archives numériques.

#### Informations supplémentaires

La norme ETSI TS 102 176-1 énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 10.1.3 Authentification à deux facteurs

#### Mesure

Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, il convient d'assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.

### Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé, par exemple une carte à puce ou une clé USB cryptographique contenant un certificat électronique d'authentification, un dispositif physique d'authentification ou des techniques de biométrie pour s'assurer de l'authentification sécurisée d'un utilisateur aux actifs techniques du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

Il convient d'utiliser un dispositif de filtrage d'adresses IP associé à un moyen cryptographique, par exemple un certificat SSL, pour s'assurer de l'authentification sécurisée d'un actif technique du système de conservation aux autres actifs du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques

### Mesure

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation avec des algorithmes et techniques cryptographiques appropriés.

### Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation pour s'assurer que ces documents sont correctement stockés, traités et supprimés et que ces archives sont correctement créées, exploitées, restituées, transférées ou supprimées.

Il convient que pour chaque document numérique à archiver, son empreinte digitale soit calculée par l'émetteur de ce document et transmise de manière sécurisée à l'organisation qui vérifiera l'intégrité du document numérique reçu en calculant et en obtenant une empreinte digitale identique à celle transmise par l'émetteur du document.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 10.1.5 Protection de l'intégrité des documents internes

### Mesure

Il convient de protéger l'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événements du SDC, avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

### Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents internes dans le temps, en particulier des journaux d'événements ou des opérations de vérification.

Il convient en particulier de s'assurer de :

a. l'établissement d'un schéma de liaison pour lier les événements enregistrés d'un journal entre eux permettant de détecter toute suppression d'événements survenus par le passé,

b. l'horodatage régulier, par exemple une fois par jour, des journaux d'événements par une autorité d'horodatage qualifiée.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 10.1.6 Signature électronique des documents internes

### Mesure

Il convient que les utilisateurs du SDC utilisent une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.

### Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé pour permettre :

a. à un utilisateur du système de conservation de signer électroniquement des rapports d'activités d'administration, d'opérations et de sécurité du système de conservation de manière à s'assurer de l'authenticité des activités effectuées,
b. à une personne de l'organisation de signer électroniquement les transmissions d'informations, de documents numériques et d'archives numériques à destination des clients (internes ou externes à l'organisation) et des autorités compétentes de manière à s'assurer de l'authenticité des envois.

Le dispositif sécurisé de création de signatures électroniques et le certificat électronique qualifié utilisé doivent répondre aux exigences définies par l'Union européenne en la matière.

Il convient également d'utiliser des formats de signatures électroniques comme CAdES [5], XAdES [6] et PAdES [7] pour maintenir une pérennité de la signature électronique, des informations, des documents numériques et des archives numériques attachés à cette signature.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 10.1.7 Protection des transmissions de documents

### Mesure

Il convient de protéger la transmission d'informations et de documents numériques avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

### Préconisations de mise en œuvre

Il convient d'utiliser un protocole sécurisé (SFTP, TLS, PPP, L2TP et IPSec…) pour sécuriser la transmission d'informations, de documents numériques et d'archives numériques entre les éléments suivants :

a. les actifs techniques du système de conservation, même pour ceux appartenant à un même réseau ;
b. les parties concernées par le processus de conservation comme l'organisation, les clients (internes ou externes à l'organisation) et les autorités compétentes.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 10.1.8 Conservation des signatures électroniques

### Mesure

Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, il convient de conserver le document avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.

### Préconisations de mise en œuvre

Il convient de démontrer l'intégrité du document en démontrant :

a. qu'au moment de l'archivage, la signature électronique était correcte, le certificat électronique qualifié y apposé était valide et issu d'une autorité de certification reconnue ;
b. que le système d'archivage conserve l'intégrité des documents archivés aussi longtemps que nécessaire.

### Informations supplémentaires

Plusieurs techniques sont possibles à cette fin comme :

a. l'utilisation du protocole de vérification en ligne de certificats (OCSP) de l'autorité de certification émettrice du certificat électronique qualifié,
b. l'horodatage du rapport d'activités signé et récupération de la liste de révocation des certificats (CRL) publiée régulièrement par l'autorité de certification émettrice du certificat électronique qualifié.

# 11 Sécurité physique et environnementale

## 11.1 Zones sécurisées

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 11.1.7 Accompagnement des visiteurs

### Mesure

Il convient qu'un membre de l'organisation habilité accompagne de manière permanente tous les visiteurs de l'organisation, même si l'accès à ces zones leur a déjà été autorisé.

### Préconisations de mise en œuvre

Il convient d'assurer que les visiteurs n'accèdent pas aux zones associées au processus de dématérialisation, notamment en cas d'activités de traitement de documents analogiques de clients pour réduire les risques de divulgation non autorisée d'informations.

Il convient de prendre les mesures nécessaires pour s'assurer que les visiteurs ne puissent pas voir des informations des clients.

Il convient d'assurer une surveillance effective des tiers autorisés de manière permanente à accéder aux zones sécurisées de l'organisation dès qu'ils accèdent aux actifs techniques du SDC et aux documents des clients.

Il convient de protéger les actifs techniques du SDC contre des accès non autorisés :

a. en cas d'évacuation des zones hébergeant ces actifs,

b. au cas où ils sont situés dans des sites multioccupants.

## 11.2 Matériels

*Des préconisations de mise en œuvre additionnelles sont :*

### 11.2.1 Emplacement et protection du matériel

#### Préconisations de mise en œuvre

Il convient de considérer les documents analogiques des clients comme des actifs nécessitant une protection spéciale (au sens de 11.2.1.d de la norme ISO/IEC 27002:2013) au niveau des conditions ambiantes et des autres menaces liées.

### 11.2.5 Sortie des actifs

#### Préconisations de mise en œuvre

Il convient de ne pas sortir de l'organisation sans autorisation préalable du client des documents analogiques du processus de dématérialisation, excepté pour prévenir la destruction de ces actifs en cas de catastrophe.

# 12 Sécurité liée à l'exploitation

## 12.1 Procédures et responsabilités liées à l'exploitation

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 12.1.5 Procédures d'exploitation du SDC

#### Mesure

Il convient de définir, mettre en œuvre, et faire suivre par le personnel concerné (de l'organisation et des fournisseurs) des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

#### Préconisations de mise en œuvre

Il convient d'inclure dans les procédures de gestion du SDC les activités suivantes :

a. la gestion des accès au SDC et des privilèges associés aux comptes du SDC ;
b. la gestion des fonctionnalités d'administration, d'opérations et de sécurité du SDC et des instructions pour les exécuter ;
c. la gestion de la configuration du SDC ;
d. l'instruction du fonctionnement du SDC en mode dégradé, de son redémarrage et de sa récupération ;
e. la gestion des mécanismes de surveillance du SDC ;
f. la gestion des journaux d'événements du SDC et des instructions pour leur exploitation ;
g. la gestion des mécanismes cryptographiques de sécurité du SDC, comme les suivants :
    1. les mécanismes d'authentification et de signature des utilisateurs du SDC,
    2. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques,
    3. les mécanismes d'intégrité des documents numériques, des archives numériques et des journaux d'événements, ainsi que

4. le remplacement de ces mécanismes en cas de découverte de vulnérabilités sans altérer l'exploitabilité et l'intégrité des archives ;

h. si c'est convenu dans l'accord avec les clients, la gestion des mécanismes de détection et de suppression de codes malveillants ;
i. gestion des mécanismes de contrôle régulier d'intégrité du SDC ;
j. gestion des mécanismes de suppression des documents numériques et des archives numériques gérées par le SDC ;
k. gestion des supports de stockage du SDC, de leur remplacement et de leur mise au rebut ;
l. gestion des sauvegardes du SDC, des sauvegardes des documents numériques et des archives numériques gérées par le SDC et de leur restauration respective ;
m. gestion de la continuité et de la reprise du SDC même en cas de désastre ;
n. gestion des changements du SDC ;
o. gestion des incidents pouvant impacter le SDC ;
p. maintenance des actifs techniques avec gestion du support des fournisseurs en cas de dysfonctionnement du SDC ;
q. gestion des métadonnées de description et de contrôle associées aux archives numériques ;

et en plus pour les processus de dématérialisation :

r. la gestion des mécanismes de vérification de l'adéquation du nombre de documents analogiques (ou du nombre de pages composant ces documents) numérisés ;
s. la gestion des mécanismes de vérification du contenu des documents numériques.

*Des préconisations de mise en œuvre additionnelles sont :*

## 12.4 Journalisation et surveillance

## 12.4.1 Journalisation des événements

### Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux tous les événements en lien avec le SDC, en particulier :

a. les événements système des actifs du SDC,
b. les erreurs et dysfonctionnements des actifs du SDC,
c. les erreurs et dysfonctionnements liés à la génération de journaux d'événements,
d. les événements liés aux documents analogiques, aux documents numériques et aux archives numériques traitées par le SDC.

## 12.4.3 Journaux administrateur et opérateur

### Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux toutes les activités effectuées par les comptes des utilisateurs du SDC, incluant les activités effectuées hors de conditions normales d'utilisation du SDC en lien avec le SDC, en particulier :

a. les tentatives de connexion d'utilisateurs hors des heures normales de bureau,
b. les activités effectuées par les utilisateurs dans un laps de temps plus court que la normale, pouvant conduire à suspecter qu'elles sont réalisées par des actifs techniques et non des personnes physiques,
c. la duplication de sessions utilisateurs.

## 12.4.4 Synchronisation des horloges

### Préconisations de mise en œuvre

Il convient d'assurer que :

a. les actifs techniques supportant le SDC soient synchronisés avec le temps universel coordonné (UTC), *via* une source de temps faisant autorité,
b. les événements liés à la synchronisation régulière de l'horloge système des actifs techniques du SDC soient enregistrés et conservés aussi longtemps que nécessaire,
c. un unique format de la date et de l'heure soit adopté pour la génération des événements du SDC pour faciliter la traçabilité des actions effectuées,
d. une synchronisation avec l'horloge maîtresse soit faite de façon suffisamment régulière pour s'assurer que la variation entre l'horloge maître et l'horloge des systèmes dans le périmètre reste en dessous du seuil d'une seconde,
e. toute variation supérieure à la variation tolérée soit détectée dans les plus brefs délais afin que des actions correctrices puissent être adoptées,
f. des éléments de vérification de l'exactitude de l'horloge, comme des jetons d'horodatage sont générés dans le cadre du fonctionnement du SDC.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 12.4.5 Exploitabilité des journaux d'événements

### Mesure

Il convient de conserver les journaux d'événements générés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.

### Préconisations de mise en œuvre

Il convient de centraliser l'information journalisée en lien avec le SDC.

Il convient d'utiliser des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire des journaux d'événements.

*Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :*

## 12.8 Gestion correcte et sécurisée du SDC

Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.

## 12.8.1 Adéquation du SDC

### Mesure

Il convient de démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

## 12.8.2 Description détaillée du SDC

### Mesure

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes.

### Préconisations de mise en œuvre

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC :

a. en identifiant et en documentant les actifs techniques supportant les processus sous-jacents au processus de dématérialisation ou de conservation, à savoir :
   1. la collecte des documents analogiques ou numériques,
   2. le stockage temporaire de ces documents,
   3. la création de documents numériques ou des archives numériques,
   4. la restitution, le transfert, la destruction éventuelle des documents analogiques, et la suppression des archives numériques ;

b. en identifiant, en évaluant et en documentant de manière régulière les aspects fonctionnels et opérationnels du SDC, comme les suivants :
   1. pour le système de dématérialisation, pour chaque scanneur :
      i. les nombres minimum et maximum de couleurs et les niveaux de gris,
      ii. les nombres minimum et maximum de dpi, de bits par pixel,
      iii. la possibilité de dématérialisation recto/verso ou uniquement verso,
      iv. les différents formats à l'entré, comme A3, A4 et A5,
      v. les méthodes de correction d'images, comme le redressement, la suppression de points isolés, et la suppression des marges,
      vi. les méthodes de compression des images,
      vii. le nombre de documents analogiques ou nombre de pages composant les documents analogiques pouvant être numérisés dans un laps de temps donné ;
   2. pour le système de conservation :
      i. le nombre maximum ou la taille maximum de documents numériques pouvant être transmis en un lot,
      ii. le débit de transmission des documents numériques ou de restitution d'archives numériques,
      iii. les délais de réponse,
      iv. la fréquence d'émission des lots ou de restitutions d'archives numériques,
      v. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques supportées, comme SFTP, TLS, PPP, $L_2TP$ et IPSec.

c. en documentant sur des schémas l'architecture du réseau, les flux de données entre les actifs, les dépendances entre les actifs.

## 12.8.3 Mécanismes de sécurité du SDC

### Mesure

Il convient de gérer et de documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.

### Préconisations de mise en œuvre

Il convient en particulier de gérer les mécanismes de sécurité suivants :

a. Mécanismes de gestion des accès au SDC.

Il convient de protéger les accès aux actifs techniques du SDC, aux documents analogiques, aux documents numériques et aux archives numériques gérés par le SDC en :

1. s'assurant que les conditions d'accès à ces actifs s'appliquent à toute personne physique et à tout actif tentant d'y accéder,
2. assurant une gestion adéquate des comptes des utilisateurs autorisés à accéder au SDC et des comptes techniques des actifs techniques du SDC, avec une capacité de révocation immédiate de ces comptes,
3. en identifiant sans ambigüité les activités et les actions système effectuées et en pouvant les attribuer de façon incontestable à un auteur, par exemple en attribuant des comptes personnels à chaque utilisateur,
4. gérant des mécanismes d'authentification appropriés et sécurisés pour les comptes des utilisateurs autorisés et les comptes techniques des actifs techniques du SDC.

b. Mécanismes de gestion des privilèges.
Il convient d'assurer une gestion des privilèges pour l'ensemble des comptes des utilisateurs du SDC et des comptes techniques des actifs techniques du SDC (voir 6.1.2 et 6.1.6).
c. Mécanismes de surveillance (voir 12.4.3).
d. Mécanismes cryptographiques de sécurité (voir 10.1).
e. Mécanismes de détection et de suppression de codes malveillants contenus dans des documents numériques collectés en vue de leur conservation électronique, si c'est demandé par le client.

Il convient d'utiliser au minimum un antivirus pour vérifier que tous les documents numériques collectés en vue de leur conservation électronique ne contiennent pas de codes malveillants, comme des virus, des chevaux de Troie et des vers de réseau.

Il convient de l'utiliser dès la réception par le SDC des documents numériques et avant le démarrage du processus de création des archives numériques.

f. Mécanismes de suppression sécurisée des documents et archives numériques, comme une réécriture multiple sur les informations ne permettant plus de les retrouver en l'état.
g. Mécanismes de conversion (si nécessaire) des archives numériques dans un format différent de leur format original.

## 12.8.4 Supervision des aspects opérationnels du SDC

### Mesure

Il convient d'évaluer de manière régulière les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants.

### Préconisations de mise en œuvre

Il convient :

a. de définir une liste avec les aspects opérationnels du SDC à contrôler ;
b. de l'inclure dans la liste des éléments nécessaires de surveiller selon les exigences de l'évaluation des performances du système de management (voir ISO/IEC 27001 2013, chapitre 9.1) ;
c. d'établir des indicateurs de disponibilité des caractéristiques opérationnelles, comme les durées de vie des disques.

## 12.8.5 Contrôle régulier de l'intégrité du SDC

### Mesure

Il convient d'implémenter des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité.

### Préconisations de mise en œuvre

En ce qui concerne le SDC, il convient de s'assurer que :

a. le fonctionnement du SDC n'a pas été altéré suite à des :
   1. opérations de maintenance ou des mises à jour,
   2. remplacements d'actifs du SDC comme les scanneurs, la plateforme de conservation électronique ou des composants de ces actifs comme les supports de stockage ;

b. les fichiers de configurations du SDC n'ont pas été modifiés de manière non autorisée ;
c. l'intégrité est préservée en ce qui concerne les
   1. documents numériques stockés,
   2. métadonnées associées,
   3. archives numériques,
   4. journaux d'événements.

## 13 Sécurité des communications

*Les objectifs, mesures, préconisations de mise en œuvre et informations supplémentaires de la norme ISO/IEC 27001:2013 s'appliquent sans modification.*

## 14 Acquisition, développement et maintenance des systèmes d'information

## 14.1 Exigences de sécurité applicables aux systèmes d'information

*Des préconisations de mise en œuvre additionnelles sont :*

### 14.1.1 Analyse et spécification des exigences de sécurité de l'information

### Préconisations de mise en œuvre

Il convient de s'assurer et de pouvoir démontrer que les applications critiques et les systèmes d'information supportant le SDC sont réalisés en respectant des méthodes de développement sécurisé reconnues.

Il convient d'évaluer et le cas échéant d'instaurer le principe de dépôts des codes source chez un tiers pour toute application du SDC fournie par un fournisseur et nécessaire à assurer l'intégrité et la disponibilité des informations.

# 15 Relations avec les fournisseurs

## 15.1 Sécurité de l'information dans les relations avec les fournisseurs

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

### 15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation

#### Mesure

Il convient d'inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation.

#### Préconisations de mise en œuvre

Pour tous les fournisseurs supportant les processus de dématérialisation ou de conservation exécutés par l'organisation, il convient d'étudier les conditions suivantes, puis d'inclure les conditions nécessaires pour maitriser les risques liés à l'activité du fournisseur, dans le document contractuel établi avec ce fournisseur :

a. des dispositions quant à la propriété des produits et des services, comme des documents et des applications, fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation ;
b. des dispositions quant à la continuité de la délivrance des produits et des services fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation, même en cas de désastre ;
c. le respect de la politique de dématérialisation ou de la politique de conservation de l'organisation ;
d. des mesures garantissant :
    1. une notification dans les plus brefs délais des changements sécuritaires appliqués aux actifs du fournisseur et de ses fournisseurs pouvant impacter les processus de dématérialisation ou de conservation exécutés par l'organisation,
    2. que les informations de l'organisation seront utilisées exclusivement pour les finalités pour lesquelles elles ont été rendues accessibles au fournisseur et à ses fournisseurs,
    3. que les changements de fournisseurs du fournisseur impliqués dans le support des processus de dématérialisation ou de conservation exécutés par l'organisation seront sujets à approbation préalable de l'organisation ;
e. l'engagement du fournisseur à coopérer avec l'organisation dans le cadre d'investigations effectuées par l'organisation pour la résolution d'un incident pouvant impacter les services ou produits fournis à l'organisation par le fournisseur et dont l'origine présumée ou avérée est autre que le fournisseur ou ses fournisseurs ;
f. le droit d'auditer les fournisseurs du fournisseur de manière équivalente à ce dernier et dans le périmètre de leur implication au niveau des processus de dématérialisation ou de conservation exécutés par l'organisation ;
g. la conformité du fournisseur et de ses fournisseurs aux lois et aux règlements en vigueur au Luxembourg ;
h. les points de contact de chaque partie concernée par le document contractuel, d'un point de vue contractuel, opérationnel et de la sécurité de l'information.

# 16 Gestion des incidents liés à la sécurité de l'information

# 16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

*Des préconisations de mise en œuvre additionnelles sont :*

## 16.1.1 Responsabilités et procédures

### Préconisations de mise en œuvre

Il convient de documenter dans une procédure les instructions précisant à partir de quel moment la gestion d'incidents est activée, la restauration est entamée et les autorités ou les clients concernés (internes ou externes à l'organisation) sont avertis de cet incident.

### Informations supplémentaires

Voir mesure 6.1.6.

# 17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

*Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :*

## 17.3 Continuité de l'activité et du SDC

Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.

## 17.3.1 Organisation de la continuité

### Mesure

Il convient de déterminer les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre.

### Préconisations de mise en œuvre

Il convient de définir pour les actifs dans le périmètre la durée maximale d'interruption admissible (DMIA) (anglais : Return Time on Objective – RTO) et la perte de données maximale admissible (PDMA) (anglais : Recovery Point Objective – RPO) en tenant compte des exigences des clients et de l'obligation de restitution des documents.

### Informations supplémentaires

La Norme internationale ISO/IEC 22301:2014 relative à la « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences » spécifie les exigences pour planifier, établir, mettre en place et en œuvre, opérer, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent. Elle permet à toute organisation, y compris à un PSDC, de concevoir un système de management de la continuité des activités qui soit adapté à ses besoins et qui satisfasse aux exigences des parties intéressées.

### 17.3.2 Mise en œuvre de la continuité

#### Mesure

Il convient d'établir, de documenter, de mettre en œuvre et de maintenir les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable.

#### Préconisations de mise en œuvre

Il convient de définir un processus de reprise d'activé qui inclut les processus de dématérialisation ou de conservation et qui tient compte des exigences des clients, de l'obligation de restitution des documents, et des scénarios de risques qui peuvent interrompre le bon fonctionnement d'une activité.

Il convient de gérer des plans de continuité pour les processus de dématérialisation ou de conservation permettant d'adresser les situations défavorables selon les conditions définies.

Il convient de gérer un plan de reprise de l'activité du SDC permettant d'adresser les situations défavorables selon les conditions définies.

### 17.3.3 Vérifier, revoir et évaluer la continuité

#### Mesure

Il convient de vérifier la mise en œuvre des mesures liées à la continuité du SDC à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

#### Préconisations de mise en œuvre

Il convient de tester les éléments clés des plans de continuité et des plans de reprises.

## 18 Conformité

## 18.1 Conformité aux obligations légales et réglementaires

*Des préconisations de mise en œuvre additionnelles sont :*

### 18.1.3 Protection des enregistrements

#### Préconisations de mise en œuvre

Il convient de conserver les preuves de la conformité des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de dématérialisation ou de conservation exécuté par l'organisation en utilisant des supports de stockage appropriés une conservation aussi longtemps que nécessaire.

En particulier il convient de conserver les preuves suivantes :

a. les rapports d'activités des utilisateurs du SDC,
b. les rapports de mises à jour ou de changement du SDC,
c. les rapports d'événements et d'incidents lié aux processus de dématérialisation ou de conservation,
d. les rapports de revue des journaux d'événements du SDC ;
e. en cas de processus de dématérialisation :
    1. les bordereaux de récupération ou de livraison de documents analogiques ;
f. en cas de processus d'archivage :
    1. les rapports de conversion de documents numériques en archives numériques,
    2. les rapports de conversion d'archives numériques en cas de changements de format.

Il convient qu'une preuve liée aux activités effectuées par le personnel concerné contienne en particulier les informations suivantes :

a. les auteurs des activités effectuées,
b. les dates et heures des activités effectuées,
c. les lieux des activités effectuées,
d. les actifs utilisés pour la réalisation de ces activités,
e. les actifs visés par ces activités,
f. le descriptif des activités effectuées,
g. les problèmes ou erreurs rencontrés pendant la réalisation de ces activités,
h. les clients (interne ou externe) concernés.

## 18.2 Revue de la sécurité de l'information

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation

### Mesure

Il convient de réaliser un audit interne de conformité du SDC afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.

### Préconisations de mise en œuvre

Il convient que cette évaluation s'assure :

a. par échantillonnage que les documents analogiques collectés ont été correctement transformés en documents numériques et par la suite détruits ou restitués, et que les documents numériques ont été correctement maintenus, restitués ou entrés dans un processus d'archivage ;
b. par échantillonnage que les documents numériques collectés ont été correctement conservés sous la forme d'archives numériques et par la suite supprimés, et que ces archives ont été correctement créées, maintenues, restituées, transférées ou supprimées ;
c. que les actifs critiques du SDC et les mécanismes de sécurité, comme les mécanismes cryptographiques, ont été évalués et certifiés par des organismes indépendants spécialisés dans ce type de revues ou qu'ils sont conformes à des normes ou des référentiels reconnus et qu'ils sont utilisés conformément aux bonnes pratiques en la matière ;
d. par échantillonnage que les procédures d'administration, d'opérations et de sécurité et des procédures d'exploitation du processus et les règles définies dans ces procédures sont respectées.

### Informations supplémentaires

La norme ISO/IEC 27007 intitulé « Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information » fournit des préconisations sur la réalisation des audits de SMSI, ainsi que des lignes directrices sur les compétences des auditeurs, en complément des lignes directrices figurant dans l'ISO 19011, qui sont applicables aux systèmes de management en général.

*Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :*

## 18.2.5 Revue indépendante de la sécurité du SDC

### Mesure

Il convient de réaliser un audit technique du SDC et des mécanismes de sécurité afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.

### Préconisations de mise en œuvre

Il convient que cet audit technique inclut des tests, en particulier des tests d'intrusion et des tests d'escalade de privilèges et une conclusion par une personne expérimentée en test d'intrusion.

### Informations supplémentaires

Le rapport technique ISO/IEC TR 27008 intitulé « Lignes directrices pour les auditeurs des contrôles de sécurité de l'information » fournit des préconisations pour la revue de la mise en œuvre et de l'exploitation des mesures de sécurité, y compris le contrôle de la conformité technique des mesures de sécurité. Il explique des techniques pouvant être utilisées pour un tel audit technique. L'audit est en général composé d'un audit de la configuration des systèmes et de l'activité du système pour vérifier le fonctionnement correct de chaque mécanisme de sécurité, d'un test d'intrusion externe, et d'un test d'escalade de privilège.

(1) ISO/IEC 27001:2013 et ISO/IEC 27002:2013.

# Annexe A (normative) : Objectifs et mesures de référence spécifiques aux PSDC

Tableau A.1 - Objectifs et mesures

| | | |
|---|---|---|
| A.5 Politique de sécurité de l'information | | |
| A.5.1 Orientation de la direction en matière de sécurité de l'information | | |
| Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. | | |
| A.5.1.1 | Politiques de sécuirité de l'information | *Mesure*<br><br>Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés. |
| QA.5.1.2 | Revue des politiques de sécurité de l'informa- | *Mesure*<br><br>Les politiques de sécurité doivent être revues à intervalles |

Les objectifs et les mesures énumérés dans le Tableau A.1 découlent directement de ceux qui sont répertoriés dans le chapitre 5, avec lesquels ils sont en adéquation, et doivent être utilisés dans le contexte du paragraphe 6.1.4. La déclaration d'applicabilité doit justifier, en utilisant la méthode retenue pour l'appréciation et de traitement des risques, l'exclusion de toutes mesures.

Il y a 4 objectifs spécifiques et 34 mesures spécifiques au PSDC dont aucune obligatoire, donc qui ne peuvent pas être exclues par le processus de traitement des risques.

## 5 Politiques de sécurité de l'information

## 5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation

| |
|---|
| Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. |

### 5.2.1 Politiques de dématérialisation ou de conservation

Une politique de dématérialisation ou de conservation doit être définie, approuvée par la direction, mise en application, diffusée et communiquée aux salariés et aux tiers concernés.

### 5.2.2 Revue de la politique de dématérialisation ou de conservation

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité de politiques des processus de dématérialisation ou de conservation, ces politiques doivent être revues à intervalles programmés et en cas de changements majeurs.

# 6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation

## 6.1 Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.

### 6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation

Toutes les responsabilités en matière de sécurité de l'information et des processus de dématérialisation ou de conservation, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables, doivent être établies et d'attribuées.

## 6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation

Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.

### 6.3.1 Vérification des documents numériques avant destruction des documents analogiques correspondants

Une vérification du contenu des documents numériques par rapport aux documents analogiques doit être exercée si la destruction de ces derniers est programmée à la suite de leur numérisation.

### 6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques

L'organisation doit s'assurer que toute modification ou suppression des archives numériques créées qui n'était pas programmée lors de la définition du projet de conservation nécessite l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

### 6.3.3 Gestion des preuves

Une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné doit être établie dans une procédure et mise en œuvre.

### 6.3.4 Relations avec l'autorité nationale

Des procédures doivent être mises en application pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de dématérialisation ou de conservation.

## 6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients

Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.

### 6.4.1 La sécurité dans les accords avec les clients

Le PSDC doit définir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.

### 6.4.2 Obligation d'information préalable du client

Préalablement à toute relation contractuelle avec un détenteur, le PSDC doit mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.

### 6.4.3 Classification des actifs du client

Le client doit définir avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.

### 6.4.4 Obligation d'information du client en cas de changements ou d'incidents

Le PSDC doit informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

## 7 La sécurité des ressources humaines

## 7.2 Pendant la durée du contrat

### 7.2.4 Engagement envers les politiques

Le personnel interne et celui des fournisseurs, s'il est impliqué dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, doivent comprendre et s'engager par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.

## 8. Gestion des actifs

## 8.1 Responsabilités relatives aux actifs

### 8.1.4 Cloisonnement d'informations secrètes ou d'informations à caractère personnel

D'éventuelles informations secrètes ou informations à caractère personnel doivent être cloisonnées de façon suffisante pour pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.

# 9 Contrôle d'accès

## 9.1 Exigences métier en matière de contrôle d'accès

### 9.1.3 Ségrégation effective liée aux droits d'accès

Trois personnes différentes doivent être impliquées dans la gestion d'un droit d'accès: une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.

# 10 Cryptographie

### 10.1.3 Mesures d'authentification à deux facteurs

Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, le PSDC doit assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.

### 10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques

L'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation doit être protégée avec des algorithmes et techniques cryptographiques appropriés.

### 10.1.5 Protection de l'intégrité des documents internes

L'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événement du SDC, doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

### 10.1.6 Signature électronique des documents internes

Les utilisateurs du SDC doivent utiliser une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.

### 10.1.7 Protection des transmissions de documents

La transmission d'informations et de documents numériques doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

### 10.1.8 Conservation des signatures électroniques

Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, le document doit être conservé avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.

# 11 Sécurité physique et environnementale

## 11.1 Zones sécurisées

### 11.1.7 Accompagnement des visiteurs

Un membre du PSDC habilité doit accompagner de manière permanente tous les visiteurs du PSDC, même si l'accès à ces zones leur a déjà été autorisé.

# 12 Sécurité liée à l'exploitation

## 12.1 Procédures et responsabilités liées à l'exploitation

### 12.1.5 Procédures d'exploitation du SDC

Des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et l'exploitabilité doivent être définies, mises en œuvre, et suivies par le personnel concerné (du PSDC et des fournisseurs).

### 12.4.5 Exploitabilité des journaux d'événements

Les journaux d'événements générés doivent être conservés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.

## 12.8 Gestion correcte et sécurisée du SDC

Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.

### 12.8.1 Adéquation du SDC

Le PSDC doit démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

### 12.8.2 Description détaillée du SDC

Une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes doit être définie et maintenue.

### 12.8.3 Mécanismes de sécurité du SDC

Le PSDC doit gérer et documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.

### 12.8.4 Supervision des aspects opérationnels du SDC

Les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants doivent être évalués de manière régulière.

### 12.8.5 Contrôle régulier de l'intégrité du SDC

Des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité doivent être implémentés.

## 15 Relations avec les fournisseurs

## 15.1 Sécurité de l'information dans les relations avec les fournisseurs

### 15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation

Le PSDC doit inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation.

## 17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

## 17.3 Continuité de l'activité et du SDC

Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.

### 17.3.1 Organisation de la continuité

Les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre doivent être déterminées.

### 17.3.2 Mise en œuvre de la continuité

Les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable doivent être établis, documentés, mis en œuvre et maintenus.

### 17.3.3 Vérifier, revoir et évaluer la continuité

La mise en œuvre des mesures liées à la continuité du SDC doit être vérifiée à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

## 18 Conformité

## 18.2 Revue de la sécurité de l'information

### 18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation

Un audit interne de conformité du SDC doit être réalisé afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description

détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.

### 18.2.5 Revue indépendante de la sécurité du SDC

Un audit technique du SDC et des mécanismes de sécurité doit être réalisé afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.