ILNAS

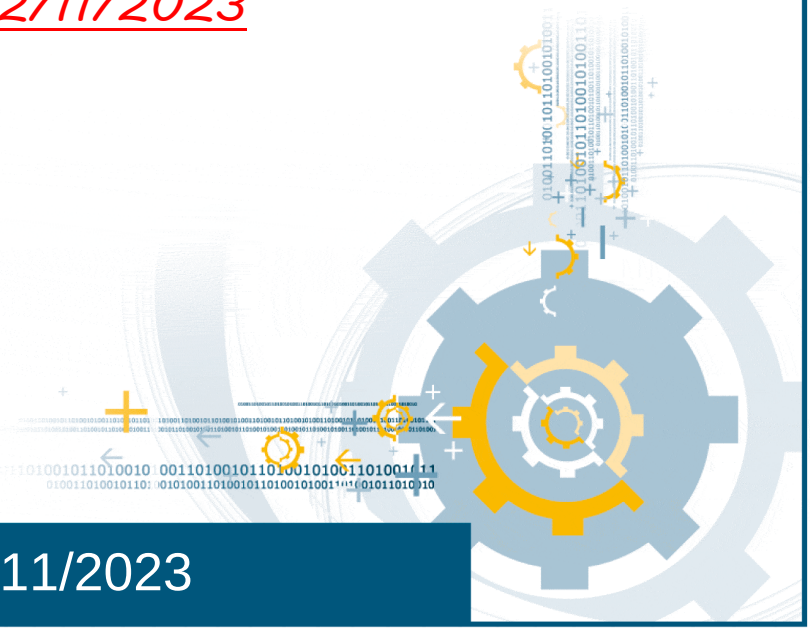
Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS 106:2023

ARCHIVAGE ÉLECTRONIQUE - RÉFÉRENTIEL D'EXIGENCES POUR LA CERTIFICATION DES PRESTATAIRES DE SERVICES DE DÉMATÉRIALISATION OU DE CONSERVATION (PSDC)

draft

02/11/2023



11/2023

Sommaire

Avant-propos

La présente norme luxembourgeoise (ILNAS 106:2023) a été élaborée par le comité technique ILNAS/TC 106 « Archivage électronique » mis en place sous la responsabilité et la présidence de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS).

La référence à cette norme luxembourgeoise devra être publiée au Journal Officiel du Grand-Duché de Luxembourg pour recevoir le statut de norme nationale.

Une attention particulière est portée au fait que certains des éléments de la présente norme peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ILNAS ne saurait être tenu responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Introduction

Contexte

La présente norme nationale (ci-après « la norme nationale ») définit des exigences et des mesures permettant à une organisation d'établir les exigences fonctionnelles et techniques de dématérialisation et conservation, ainsi qu'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 norme nationale se base sur les Normes internationales ISO/IEC 27001:2022, ISO/IEC 27002:2022 et ISO 14641:2018 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 27001:2022 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 27002:2022 et spécifiques aux processus de dématérialisation ou de conservation,

c) des processus opérationnels sécurisés de dématérialisation et de conservation.

La norme nationale peut aussi être 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 recommandations fournies dans cette norme nationale. Toute déviation par rapport à ces recommandations, 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.

La norme nationale 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.

Structure du document

Ce document est structuré de la façon suivante :

- Le chapitre 1 précise le domaine d'application de la norme nationale.
- Le chapitre 2 cite des références normatives, c'est-à-dire les normes à respecter par les organisations mettant en application la norme nationale.
- Le chapitre 3 définit les termes utilisés dans ce texte.
- Le chapitre 4 détermine les liens entre cette norme nationale et certaines normes internationales.
- Le chapitre 5 décrit les exigences spécifiques concernant la conservation des documents, à lire comme un complément à la norme internationale ISO 14641:2018 « Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques – Spécification ».
- Le chapitre 6 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 27001:2022 « Sécurité de l'information, cybersécurité et protection de la vie privée — 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 27001:2022.

- Le chapitre 7 définit des guidances spécifiques, en particulier des objectifs, des mesures de sécurité, des recommandations et des informations complémentaires. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27002:2022 « Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information », d'où la numérotation non linéaire des exigences.
- L'Annexe A résume les mesures de sécurité spécifiques énoncés au Chapitre 7 tout en les rendant leur examen obligatoire dans le traitement des risques.

Le document ne détaille pas les exigences inhérentes à la dématérialisation et à la conservation proprement dites, pour lesquelles il conviendra de se reporter aux exigences fonctionnelles et techniques de l'ISO14641:2018 « Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques – Spécification ».

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 norme nationale 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 norme nationale 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 numérique d'un document analogique sera présumée être conforme à l'original et préserver sa force probante si elle est le résultat d'un processus de dématérialisation d'un PSDC. De même, une archive numérique issue de documents numériques originaux ou d'une copie numérique, sera présumée être conforme à l'original numérique et conserver sa force probante si elle est conservée par le processus de conservation 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 norme nationale d'exigences et de mesures des PSDC est applicable à toute organisation publique ou privée.

La norme nationale a été définie à partir de Normes internationales publiées et maintenues par l'Organisation Internationale de Normalisation (ci-après « ISO »), notamment les normes :

- ISO 14641:2018 pour les exigences relatives à l'« Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques – Spécification »
- ISO 27001:2022 : les chapitres 6, 7 et annexe A de la présente norme nationale doivent donc être considérées comme un supplément aux normes ISO/IEC 27001:2022 et ISO/IEC 27002:2022 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 norme nationale.

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 14641:2018, *"Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques - Spécification"*

ISO/IEC 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*

ISO/IEC 27001:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences*

ISO/IEC 27002:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information*

3 Termes et définitions

Pour les besoins de la norme nationale, 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 universel coordonné

Pour les besoins de la norme nationale, les termes et définitions fournis dans la norme ISO/IEC 27000:2018 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.

3.3
archive

ensemble des documents quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale ou par tout service ou organisme public ou privé, dans l'exercice de leur activité

Note : Définition adaptée de la norme ISO 14641:2018, définition 3.2.

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 27000:2018]

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 27000:2018]

3.7
copie à valeur probante

une reproduction fidèle et durable sous forme numérique d'un original

3.8
conservation (électronique)

ensemble des actions visant à identifier, recueillir, classer, conserver, communiquer et restituer des documents électroniques, pour la durée nécessaire à la satisfaction des obligations légales ou pour des besoins d'informations ou à des fins patrimoniales

Note 1 : Dans la suite du document, le terme « conservation » est synonyme de « conservation électronique », sauf précision contraire.

Note 2 : Définition adaptée de la norme ISO 14641:2018, définition 3.13

3.9
dématérialisation

conversion de documents (support papier, microforme ~~ou enregistrement audiovisuel analogique)~~ en représentation codée numériquement dans un but de conservation ou de traitement de ces représentations

Note 1 : Dans la suite du document, le terme « dématérialisation » est synonyme de « copie dématérialisée à valeur probante », sauf indication contraire.

Note 2 : Définition adaptée de la norme ISO 14641:2018, définition 3.18

3.10
disponibilité

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

[ISO/IEC 27000:2018]

3.11
document

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

[ISO 15489 -1:2001]

3.12
fiabilité

propriété relative à un comportement et des résultats prévus et cohérents

[ISO/IEC 27000:2018]

3.13
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 ».

3.14
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.

3.15
intégrité

propriété d'exactitude et de complétude

[ISO/IEC 27000:2018]

3.16
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.

3.17
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 27000:2018]

3.18
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 27000:2018]

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

3.19
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 relative à l'archivage électronique, Article 2 h]

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.

3.20
preuve

information 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.

3.21
processus

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

[ISO 9000:2015]

3.22
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 27000:2018]

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.

3.23
système

ensemble d'actifs techniques corrélés ou interactifs

3.24
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

3.25
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

3.26
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 lien avec les normes existantes

Les exigences de la norme nationale PSDC définies ci-après sont d'une part, issues de normes existantes et d'autre part, des exigences définies spécifiquement pour le PSDC.

La norme nationale PSDC comprend et englobe donc :

a. Les exigences de la norme ISO 14641:2018 « Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques – Spécification », reprises dans leur intégralité (développant les exigences concernant les processus opérationnels sécurisés de dématérialisation et de conservation),

b. Les exigences de la norme ISO/IEC 27001:2022, reprises dans leur intégralité (y inclus l'Annexe A),

c. Des exigences supplémentaires à la norme ISO/IEC 27001:2022, étendant les exigences de cette norme pour y inclure les aspects de système de management de la sécurité des processus de dématérialisation et de conservation.

5 Exigences spécifiques pour PSDC relatives à la norme ISO 14641:2018

Les exigences de la norme ISO 14641:2018 s'appliquent entièrement (sauf exception dûment annoncée). Un PSDC doit donc implémenter toutes les exigences de la norme ISO 14641:2018, exceptée l'exigence 5.5.8 (demandant qu'une copie soit écrite sur un média non altérable).

Spécifiquement :

a. La clause 13 doit s'appliquer, le PSDC étant un « Trusted third-party archival »

b. Les exigences additionnelles suivantes doivent être appliquées (cf. Table 1 de la norme ISO 14641:2018):

    1. niveau de sécurité avancé (Advanced security level),

    2. authentification forte,

    3. horodatage depuis une autorité de confiance,

    4. signature électronique et horodatage des attestations des opérations et événements (unitairement ou en lot),

    5. protection contre les risques d'inondation, incendie, etc.,

    6. si nécessaire pour les besoins des clients – conversion de format planifiée et traçable,

c. si le PSDC souhaite proposer un service de dématérialisation, les clauses 5.4.2, 10.2, 10.3 et 10.4 doivent s'appliquer entièrement.

6 Exigences spécifiques pour PSDC et complémentaires à la norme ISO/IEC 27001:2022

6.1 Structure de cette norme

Cette norme est liée à la norme ISO/IEC 27001:2022 : un PSDC doit implémenter toutes les exigences de la norme ISO/IEC 27001:2022, ainsi que les exigences spécifiques étendues développées dans ce chapitre et dans l'Annexe A ; le chapitre 7 comprend le code de bonnes pratiques permettant de mettre en œuvre les exigences étendues de l'Annexe A de cette norme.

Les mesures de sécurité spécifiques sont indiqués dans l'Annexe A.

6.2 Exigences spécifiques aux systèmes de management des PSDC

Toutes les exigences des chapitres 4 à 10 de la norme ISO/IEC 27001:2022 qui ne figurent pas ci-dessous restent applicables sans modification.

4 Contexte de l'organisation

L'exigence 4.3 de la norme ISO/IEC 27001:2022 est complétée de la façon suivante.

4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

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'application.

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 27001:2022 est :

4.5 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.

Une exigence additionnelle à la norme ISO/IEC 27001:2022 est :

4.6 L'authenticité, la fiabilité, et l'exploitabilité

En complément des propriétés de sécurité de base qui sont

e. la confidentialité,
f. l'intégrité, et
g. la disponibilité,

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

h. l'authenticité (souvent considérée 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.

i. 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.

j. 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 27001:2022 limité à la sécurité de l'information, à un système de management de toutes les propriétés requises aux activités de dématérialisation ou de conservation. Il est possible de gérer, dans un SMSI, ces critères comme étant des extensions ou des combinaisons des critères particuliers de la sécurité de l'information (par exemple authenticité est un critère qui peut être considéré comme une extension à l'intégrité, la fiabilité comme extension à l'intégrité également, l'exploitabilité comme une combinaison d'extension à l'intégrité et à la confidentialité).

5 Leadership

Une exigence additionnelle à la norme ISO/IEC 27001:2022 est :

5.4 Rôles, responsabilités et autorités concernant 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 le déroulement adéquat des processus de dématérialisation ou de conservation ;
i. gérer les risques pouvant impacter le déroulement adéquat des processus de dématérialisation ou de conservation ;
j. évaluer l'adéquation des mesures adoptées en vue de mitiger les risques pouvant impacter le déroulement adéquat des processus de dématérialisation ou de conservation, et jugées non acceptables par la direction de l'organisation ;
k. gérer les preuves liées aux processus de dématérialisation ou de conservation, en adéquation avec les risques acceptés par l'organisation ;
l. évaluer les dispositifs 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 (par exemple une couverture d'assurance) ;
m. 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 ;
n. sensibiliser le personnel (de l'organisation et des tiers) concerné quant aux risques ;
o. identifier et évaluer les problèmes et les incidents ;
p. 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 27001:2022 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'application, cette politique et toutes les exigences y relatives ne sont 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 d'une situation financière suffisante et d'une situation stable pour répondre aux attentes des parties intéressées à l'activité de PSDC ;

   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,
- niveau d'exposition des activités métiers aux facteurs externes à l'organisation,
- rapport d'auditeurs financiers.

j. 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 ou les sous-processus de restitution, transfert et suppression des archives numériques permettant de gérer les risques liés à la cessation partielle ou complète d'activités

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.

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.

6 Planification

Une exigence additionnelle à la norme ISO/IEC 27001:2022 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. intégrer les preuves et leur gestion dans son processus d'identification (6.1.2 c), d'analyse (6.1.2.d) et d'évaluation des risques (6.1.2.e) ;

c. appliquer son processus de traitement des risques de sécurité aux risques déterminés aux points précédents ;

d. comparer les mesures de sécurité 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 ;

e. compléter la déclaration d'applicabilité déterminée en 6.1.3 d) avec les mesures de l'Annexe A du présent document et la justification de leur insertion ou de leur exclusion, ainsi que, le cas échéant, l'indication de leur mise en œuvre ;

f. porter à connaissance des clients et à l'autorité nationale (si nécessaire) la déclaration d'applicabilité, notamment si elle contient des exclusions.

7 Support

Une exigence additionnelle à la norme ISO/IEC 27001:2022 est :

7.6 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 matière de dématérialisation ou de conservation et concernant les processus de dématérialisation ou de conservation.

8 Fonctionnement

Une exigence additionnelle à la norme ISO/IEC 27001:2022 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 de la performance

L'exigence 9.1 de la norme ISO/IEC 27001:2022 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 27001:2022 est complétée de la façon suivante.

9.2.3 Audit interne du système de management des processus de dématérialisation et de conservation

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 réguliers et 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 norme nationale ;

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 27001:2022 est complétée de la façon suivante.

9.3.4 Revue du système de management des processus de dématérialisation ou de conservation

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 considération :

h. 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.

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, des clients, des utilisateurs ;
3. de nature légale et réglementaire ayant un impact sur les activités et les processus de l'organisation.

10 Amélioration

L'exigence 10.1 de la norme ISO/IEC 27001:2022 est complétée de la façon suivante.

10.1 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.

7 Mesures de sécurité spécifiques aux PSDC en relation avec ISO/IEC 27002:2022

Tous les objectifs de sécurité, mesures de sécurité, recommandations, et informations supplémentaires de la norme ISO/IEC 27002:2022 qui ne figurent pas ci-dessous restent applicables sans modification.

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

5 Mesures de sécurité organisationnelles

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 5.9 sont :

5.9 Inventaire des informations et autres actifs associés

Recommandations

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.

Propriété

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

a. approuve l'évaluation des aspects opérationnels du SDC au moins une fois par an et suite à une modification significative ;
b. revoit 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.

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 5.24 sont :

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

Recommandations

Il convient de documenter dans une procédure les instructions précisant les modalités d'activation de la gestion d'incidents, de la restauration et de la communication aux autorités ou aux clients concernés (internes ou externes à l'organisation) de cet incident.

Des mesures de sécurité additionnelles à la norme ISO/IEC 27002:2022 sont :

5.38 Politique de dématérialisation ou de conservation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Identifier	#Gouvernance	#Gouvernance_et_Écosystème #Résilience

Mesure de sécurité

Il convient de définir une « politique de dématérialisation ou de conservation » et de :

- la faire approuver par la direction ;
- de la mettre en application ;
- de la diffuser et la communiquer aux salariés et aux tiers concernés.

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.

Recommandations

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 de la politique d'archivage décrite en Annexe A de l'ISO 14641:2018, appliqués aux processus de dématérialisation ou de conservation, complétés par les éléments suivants :

a. une présentation de l'organisation, de son historique et de ses activités métiers ;
b. un 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. 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 propriétés de la sécurité de l'information appliquées 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. les modalités de revue de la politique de dématérialisation ou de conservation.

Une description des éléments principaux de cette politique est décrite en Annexe B.

Informations supplémentaires

Pas d'informations supplémentaires.

5.39 Revue de la politique de dématérialisation ou de conservation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Identifier #Répondre	#Gouvernance	#Gouvernance_et_Écosystème #Résilience

Mesure de sécurité

Il convient de revoir la politique de dématérialisation ou de conservation et les processus y relatifs à intervalles programmés et en cas de changements majeurs.

Objectif

Garantir la constance de la pertinence, de l'adéquation et de l'efficacité de la politique de dématérialisation ou de conservation.

Recommandations

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

Il convient notamment de considérer comme changements majeurs :

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.

Informations supplémentaires

Pas d'informations supplémentaires.

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

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Identifier #Protéger	#Gouvernance	#Gouvernance_et_Écosystème #Résilience

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.

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

Recommandations

Il convient d'attribuer les responsabilités conformément à la politique de sécurité de l'information (voir 5.1 de l'ISO/IEC 27002:2022) et à la politique de dématérialisation ou de conservation (voir 5.38 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 ou moyens de traitement de l'information.

Il convient de déterminer les responsabilités relatives à la gestion des preuves.

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

a. il convient d'identifier et de définir 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 son rôle et ses responsabilités à un niveau de détail proportionnel au risque qui y est associé (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 :

f. la gestion de la documentation (politiques, procédures) supportant ces processus ;
g. leur définition au niveau opérationnel, incluant le SDC et les mécanismes de sécurité associés ;
h. la supervision de leur mise en œuvre ;
i. la définition de leurs critères de performances ;
j. leur évaluation selon les critères de performances ;
k. 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.

5.41 Principe du double contrôle pour la modification ou la suppression d'archives numériques

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Intégrité	#Protéger	#Gouvernance #Protection_des_informations	#Gouvernance_et_Écosystème #Protection #Résilience

Mesure

Il convient de s'assurer que toute modification ou suppression des archives numériques créées, qui n'était pas prévue contractuellement, nécessite l'approbation de deux utilisateurs autorisés à exécuter ces opérations et soit pourvue de mécanisme de non-répudiation.

Objectif

Assurer l'intégrité des archive numériques, ainsi que l'authenticité des opérations effectuées, en cas de modification ou de suppression qui n'étaient pas prévues contractuellement.

5.42 Analyse de preuves

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive #Détective	#Confidentialité #Intégrité	#Identifier #Détecter	#Assurance_de_sécurité_de_l'information #Protection_des_informations #Réglementation_et_conformité	#Gouvernance_et_Écosystème

Mesure

Il convient déterminer les preuves basées sur les caractéristiques de sécurité qui doivent être conservées et gérées par le système, prouvant le bon fonctionnement du SDC et des activités du personnel concerné, et incluant la période de rétention de ces preuves.

Objectif

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

Recommandations

Il convient de considérer au minimum les preuves suivantes :

a. preuves liées à la dématérialisation du document analogique (notamment la provenance du document analogique, la date et l'heure de la dématérialisation, le canal de réception, la localisation, les acteurs impliqués dans la dématérialisation tels l'opérateur de numérisation et le superviseur, la vérification de l'adéquation entre le document analogique et le document numérique dématérialisé) ;

b. preuves liées à l'ingestion du document numérique (notamment la provenance du document numérique, la date et l'heure, le canal de réception, la localisation, la vérification de l'adéquation entre le document envoyé et le document reçu) ;
c. preuves liées à la gestion des archives numériques (notamment la vérification périodique d'intégrité, les modifications apportées aux métadonnées ou aux archives) ;
d. preuves liées à la préservation des archives numériques (notamment la migration de format) ;
e. preuves liées à la destruction des documents analogiques, documents numériques et archives numériques ;
f. preuves liées à l'organisation (procès-verbaux de réunion, enregistrements liés à des processus non-techniques, courriers, emails de validation…)
g. preuves liées à l'opération des systèmes (traces et logs systèmes ou applicatifs, logs d'audit…) ;

Il convient de définir le lien entre les différentes preuves ainsi que la raison de leur conservation.

Il convient de déterminer la localisation des preuves, ainsi que les utilisateurs pouvant y accéder (et éventuellement les modifier).

Il convient de définir la période de rétention minimale des preuves à deux cycles de certification.

Il convient que le niveau de détail des preuves doit être proportionnel aux risques rencontrés, et clairement documenté. La durée de conservation des preuves les plus détaillées peut différer des preuves les moins détaillées.

5.43 Notifications aux autorités compétentes

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Corrective	#Confidentialité #Intégrité #Disponibilité	#Répondre #Rétablir	#Gouvernance	#Gouvernance_et_Écosystème #Résilience

Mesure

Il convient de définir et de mettre en application des procédures pour notifier aux autorités compétentes 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.

Objectif

Établir un cadre de gestion pour assurer que les autorités compétentes soient tenues informées de changements et d'incidents significatifs.

Recommandations

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. un déménagement des processus,
d. une modification du périmètre d'activités gérées par des fournisseurs impactant les processus de dématérialisation ou de conservation exécutés par l'organisation.

5.44 Ségrégation effective liée aux droits d’accès

Type de mesure de sécurité	Propriétés de sécurité de l’information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Protéger	#Assurance_de_sécurité_de_l'information #Configuration_sécurisée #Gouvernance #Gestion_des_identités_et_des_accès #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications	#Gouvernance_et_Écosystème #Protection

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.

Objectif

Établir un cadre de gestion pour les droits d’accès.

Recommandations

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.

5.45 Revue indépendante de la sécurité du SDC

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive #Corrective	#Confidentialité #Intégrité	#Détecter #Répondre #Rétablir	#Assurance_de_sécurité_de_l'information #Configuration_sécurisée #Gestion_des_identités_et_des_accès #Gestion_des_menaces_et_des_vulnérabilités #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications	#Protection #Défense #Résilience

Mesure de sécurité

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 indiqués dans la description détaillée du SDC.

Objectif

Assurer la confidentialité et l'intégrité des documents numériques à archiver et des archives numériques par une revue indépendante des mécanismes de sécurité du SDC.

Recommandations

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.

6 Mesures de sécurité applicables aux personnes

Une mesure de sécurité additionnelle à la norme ISO/IEC 27002:2022 est :

6.9 Engagement envers les politiques

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Protéger #Détecter #Répondre #Rétablir	#Assurance_de_sécurité_de_l'information #Gouvernance #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications #Sécurité_des_relations_fournisseurs	#Gouvernance_et_Écosystème #Protection #Résilience

Mesure de sécurité

Il convient que le personnel interne ainsi que 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.

Objectif

Assurer le respect de la politique de sécurité et de la politique de dématérialisation ou de conservation par le personnel interne ainsi que des fournisseurs impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation.

Recommandations

Il convient que le personnel interne ainsi que 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.

7 Mesures de sécurité physique

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 7.8 sont :

7.8 Emplacement et protection du matériel

Recommandations

Il convient de considérer les documents analogiques des clients comme des actifs nécessitant une protection spéciale au niveau des conditions ambiantes et des autres menaces liées.

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 7.10 sont :

7.10 Supports de stockage

Recommandations

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

Une mesure de sécurité additionnelle à la norme ISO/IEC 27002:2022 est :

7.15 Accompagnement des visiteurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Protéger #Détecter	#Assurance_de_sécurité_de_l'information #Protection_des_informations #Sécurité_physique #Sécurité_système_et_réseau #Sécurité_des_applications	#Protection

Mesure de sécurité

Il convient qu'un membre habilité de l'organisation accompagne de manière permanente tous les visiteurs et tiers de l'organisation qui accèdent aux zones associées au processus de dématérialisation ainsi qu'aux actifs techniques de SDC, même si l'accès à ces zones leur a déjà été autorisé.

Objectif

Assurer la confidentialité des documents analogiques, des documents numériques à archiver et des documents archivés lors de la présence de visiteurs.

Recommandations

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.

8 Mesures de sécurité technologiques

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 8.17 sont :

8.17 Synchronisation des horloges

Recommandations

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 (il convient que la période minimale de conservation soit équivalente à deux cycles de certification),
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 le temps universel coordonné soit faite de façon suffisamment régulière pour s'assurer que la variation entre le temps universel coordonné et l'horloge système des actifs techniques supportant le SDC reste en dessous du seuil d'une seconde,
e. toute variation supérieure à la variation tolérée par le SDC soit détectée dans les plus brefs délais afin que des actions correctrices puissent être adoptées.

Des recommandations additionnelles pour ISO/IEC 27002:2022, mesure 8.24 sont :

8.24 Utilisation de la cryptographie

Recommandations

En cas d'utilisation de la cryptographique, il convient de prendre en considération 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 119 312 énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

Des mesures additionnelles à la norme ISO/IEC 27002:2022 sont :

8.35 Authentification à deux facteurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité #Disponibilité	#Protéger	#Assurance_de_sécurité_de_l'information #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications	#Protection

Mesure de sécurité

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. Il convient d'effectuer une authentification à deux facteurs de ces personnes.

Objectif

Protéger les actifs techniques du système de conservation, les documents numériques à archiver et les archives numériques contre des accès non autorisés et assurer l'authenticité des opérations effectuées par les personnes qui interagissent avec le système de conservation.

Recommandations

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.

Informations supplémentaires

Pas d'informations supplémentaires.

8.36 Protection de l'intégrité des documents numériques ou des archives numériques

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Intégrité	#Protéger	#Protection_des_informations	#Protection

Mesure de sécurité

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.

Objectif

Assurer l'intégrité des documents numériques à archiver et des archives numériques.

Recommandations

Il convient que pour chaque document numérique à archiver, sa valeur de hachage 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 valeur identique à celle transmise par l'émetteur du document.

Si la protection de l'intégrité des documents numériques et des archives numériques est basée sur du hachage, il convient de signer électroniquement, cacheter électroniquement, ou d'horodater les valeurs de hachage ensemble avec les identifiants des documents correspondants. Il convient d'inclure ces valeurs de hachage et ces signatures électroniques, cachets électroniques ou jetons d'horodatage dans le contrôle régulier de l'intégrité du SDC. Il convient d'utiliser des signatures électroniques qualifiées, des cachets électroniques qualifiés, ou un service d'horodatage qualifié.

Informations supplémentaires

Pas d'informations supplémentaires.

8.37 Protection de l'intégrité des documents internes

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Intégrité	#Protéger	#Assurance_de_sécurité_de_l'information #Protection_des_informations	#Protection

Mesure de sécurité

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.

Objectif

Garantir l'intégrité dans le temps des documents internes nécessaires pour le fonctionnement des processus de dématérialisation ou de conservation.

Recommandations

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 l'horodatage régulier, par exemple une fois par jour, des journaux d'événements en utilisant un service d'horodatage qualifié.

Informations supplémentaires

Pas d'informations supplémentaires.

8.38 Signature électronique des documents internes

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive #Détective	#Confidentialité #Intégrité #Disponibilité	#Protéger #Détecter	#Assurance_de_sécurité_de_l'information #Protection_des_informations #Sécurité_physique #Sécurité_système_et_réseau #Sécurité_des_applications	#Protection

Mesure de sécurité

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.

Objectif

Assurer l'authenticité et la non-répudation des opérations effectuées par le personnel impliqué dans les processus de dématérialisation ou de conservation.

Recommandations

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 de création de signature électronique qualifié et le certificat électronique qualifié utilisé doivent répondre aux exigences définies par l'Union européenne en la matière.

Informations supplémentaires

Pas d'informations supplémentaires.

8.39 Protection des transmissions de documents

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité	#Protéger	#Assurance_de_sécurité_de_l'information #Protection_des_informations	#Protection

Mesure de sécurité

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

Objectif

Garantir la confidentialité d'informations, des documents numériques à archiver et des archives numériques durant des transmissions par voie électronique et par support physique.

Recommandations

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.

Dans le cadre d'une transmission par support physique, il convient de chiffrer les informations et de sécuriser et tracer la transmission du support.

Informations supplémentaires

Pas d'informations supplémentaires.

8.40 Protection des technologies cryptographiques

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Confidentialité #Intégrité	#Protéger #Détecter #Répondre #Rétablir	#Assurance_de_sécurité_de_l'information #Continuité #Gestion_des_menaces_et_des_vulnérabilités #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications	#Protection #Défense #Résilience

Mesure de sécurité

Il convient de protéger les technologies cryptographiques utilisées dans le SDC contre l'obsolescence technique et les vulnérabilités futures pour aussi longtemps que nécessaire.

Objectif

Garantir que les technologies cryptographiques utilisées dans le SDC répondent à leurs objectifs pour aussi longtemps que nécessaire.

Recommandations

Pour les signatures électroniques, il convient de conserver le document avec une preuve que la signature est valide, c.-à-d. que la signature électronique est correcte et que le certificat électronique qualifié y apposé était valide au moment de la signature et issu d'une autorité de certification reconnue.

Il convient d'horodater les signatures électroniques en utilisant un service d'horodatage qualifié.

Il convient de faire évoluer ou changer une fonction de hachage avant qu'elle ne devienne faible.

Il convient de renouveler les jetons d'horodatage avant qu'un des algorithmes cryptographiques utilisés pour l'horodatage devienne faible ou un des certificats utilisés pour l'horodatage expire.

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,
c. Implémentation d'un processus de renouvellement de jetons d'horodatage et de hachage tel que décrit dans RFC 4998.

La norme ETSI TS 119 312 énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

8.41 Supervision des aspects opérationnels du SDC

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Disponibilité	#Détecter #Répondre #Rétablir	#Continuité #Gestion_des_actifs	#Résilience

Mesure de sécurité

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

Objectif

Assurer la disponibilité et l'exploitabilité du SDC, ainsi que des documents numériques et archives numériques.

Recommandations

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 27001:2022, chapitre 9.1) ;
c. d'établir des indicateurs de disponibilité des caractéristiques opérationnelles, comme les durées de vie des disques.

8.42 Contrôle régulier de l'intégrité du SDC

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive #Détective	#Confidentialité #Intégrité	#Protéger #Détecter	#Assurance_de_sécurité_de_l'information #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications	#Assurance_de_sécurité_de_l'information #Configuration_sécurisée #Protection_des_informations #Sécurité_système_et_réseau #Sécurité_des_applications

Mesure de sécurité

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

Objectif

Garantir l'intégrité du SDC et des archives numériques.

Recommandations

En ce qui concerne le SDC, il convient de s'assurer régulièrement 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 tous les
    1. documents numériques stockés,
    2. métadonnées associées,
    3. archives numériques, et
    4. journaux d'événements.

Informations supplémentaires

Pas d'informations supplémentaires.

8.43 Mécanismes pour la dématérialisation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Préventive	#Intégrité	#Protéger #Détecter #Répondre #Rétablir	#Protection_des_informations	#Protection #Défense #Résilience

Mesure de sécurité

Il convient d'implémenter des mécanismes permettant au SDC d'assurer une dématérialisation conforme à l'original, si la dématérialisation fait partie du périmètre du SDC.

Objectif

Assurer l'intégrité et l'authenticité des documents numériques résultant de la dématérisalisation de documents analogiques.

Recommandations

Il convient de définir, d'implémenter et de maintenir :

a. La vérification de la complétude de l'opération de numérisation ;
b. La vérification de l'intégrité des documents numérisés ;
c. Le stockage des informations spécifiques à chaque lot numérisé ;
d. Le stockage des informations de chaque document numérisé en termes d'horodatage, d'information sur les DPI, la couleur, le format, la taille ;
e. Le contrôle qualité des documents numérisés, en suivant par exemple la norme ISO 2859 ;
f. Les opérations de conversion de format ;
g. L'adjonction des métadonnées aux documents numérisés et lots.

Informations supplémentaires

Des informations plus détaillées sur l'activité de dématérialisation se trouvent en Annexe C.

Annexe A
(normative)

Mesures de sécurité spécifiques aux PSDC

Les mesures énumérés dans le Tableau A.1 découlent directement de ceux qui sont répertoriés dans le chapitre 7, avec lesquels ils sont en adéquation, et doivent être utilisés dans le contexte de l'exigence 6.1.4 du chapitre 6 du présent document. La déclaration d'applicabilité doit justifier, en utilisant la méthode retenue pour l'appréciation et de traitement des risques, l'exclusion de toutes mesures.

Tableau A.1 – Mesures de sécurité

A.5 Mesures de sécurité organisationnelles		
A.5.38	Politique de dématérialisation ou de conservation	**Mesure de sécurité** 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.
A.5.39	Revue de la politique de dématérialisation ou de conservation	**Mesure de sécurité** La politique de dématérialisation ou de conservation et les processus y relatifs doivent être revus à intervalles programmés et en cas de changements majeurs.
A.5.40	Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation	**Mesure de sécurité** Toutes les responsabilités en matière de sécurité de l'information et des processus de dématérialisation ou de conservation doivent être définies et attribuées, 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.
A.5.41	Principe du double contrôle pour la modification ou la suppression d'archives numériques	**Mesure de sécurité** Toute modification ou suppression des archives numériques créées, qui n'était pas prévue contractuellement, nécessite l'approbation de deux utilisateurs autorisés à exécuter ces opérations et doit être pourvue de mécanisme de non-répudiation.
A.5.42	Analyse de preuves	**Mesure de sécurité** Les preuves basées sur les caractéristiques de sécurité qui doivent être conservées et gérées par le système, prouvant le bon fonctionnement du SDC et des activités du personnel concerné, doivent être définies, ensemble avec la période de rétention de ces preuves.
A.5.43	Notifications aux autorités compétentes	**Mesure de sécurité** Des procédures doivent être définies et mises en application pour notifier aux autorités compétentes 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.

A.5.44	Ségrégation effective liée aux droits d'accès	**Mesure de sécurité** 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.
A.5.45	Revue indépendante de la sécurité du SDC	**Mesure de sécurité** 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 indiqués dans la description détaillée du SDC.
A.6 Mesures de sécurité applicables aux personnes		
A.6.9	Engagement envers les politiques	**Mesure de sécurité** 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, doivent comprendre et s'engager par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.
A.7 Mesures de sécurité physique		
A.7.15	Accompagnement des visiteurs	**Mesure de sécurité** Un membre habilité de l'organisation doit accompagner de manière permanente tous les visiteurs et tiers de l'organisation qui accèdent aux zones associées au processus de dématérialisation ainsi qu'aux actifs techniques de SDC, même si l'accès à ces zones leur a déjà été autorisé.
A.8 Mesures de sécurité technologiques		
A.8.35	Authentification à deux facteurs	**Mesure de sécurité** Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques doit être assurée. Il convient d'effectuer une authentification à deux facteurs de ces personnes.
A.8.36	Protection de l'intégrité des documents numériques ou des archives numériques	**Mesure de sécurité** 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.
A.8.37	Protection de l'intégrité des documents internes	**Mesure de sécurité** L'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événements du SDC, doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.
A.8.38	Signature électronique des documents internes	**Mesure de sécurité** 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.
A.8.39	Protection des transmissions de documents	**Mesure de sécurité** La transmission d'informations et de documents numériques doit

		être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.
A.8.40	Protection des technologies cryptographiques	**Mesure de sécurité** Les technologies cryptographiques utilisées dans le SDC doivent être protégées contre l'obsolescence technique et les vulnérabilités futures pour aussi longtemps que nécessaire.
A.8.41	Supervision des aspects opérationnels du SDC	**Mesure de sécurité** Les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants doivent être évalués de manière régulière.
A.8.42	Contrôle régulier de l'intégrité du SDC	**Mesure de sécurité** Des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité doivent être implémentés.
A.8.43	Mécanismes pour la dématérialisation	**Mesure de sécurité** Des mécanismes permettant au SDC d'assurer une dématérialisation conforme à l'original doivent être implémentés, si la dématérialisation fait partie du périmètre du SDC.

Annexe B
(informative)

Politique de dématérialisation ou de conservation

Une politique de dématérialisation ou de conservation définit le domaine d'application des processus de dématérialisation ou de conservation et les objectifs de l'organisation. Elle définit les exigences du Système de Management de la Sécurité de l'Information en des termes légaux, fonctionnels, opérationnels, techniques et sécurité.

Une politique de dématérialisation ou de conservation fait partie intégrant du Système de Management de la Sécurité de l'Information. Elle permet aux différents partis impliqués (interne ou externe) d'avoir une description claire des engagements de l'organisation vis-à-vis des services de dématérialisation ou de conservation.

Elle devrait notamment inclure :

a. Les modalités de revue de la politique ;

b. Le contexte de l'organisation et de ses activités de dématérialisation ou de conservation, incluant son historique et sa stratégie ou sa motivation d'implémenter ces activités ;

c. Le cadre légal applicable à ces activités, ainsi que le niveau de conformité aux normes et référentiels reconnus du Système de Management de la Sécurité de l'Information ;

d. Une description des services de dématérialisation ou de conservation fournis, incluant le domaine d'application, les niveaux de services, du format de documents et conditions d'opérations ;

e. Les parties impliquées dans la performance des services, incluant les fournisseurs dès qu'une activité du processus est sous-traitée, et les obligations qui leur incombent ;

f. Une description des processus de dématérialisation ou de conservation, incluant leurs périmètres, niveaux de service, et moyens mis en place pour la réalisation de ces processus, même si ces processus sont effectués par des tiers ;

g. Une description des conditions et fréquences d'exécution des processus de dématérialisation ou de conservation, et une description du plan de communication ;

h. Une description des systèmes et flux d'information en place pour délivrer les services de dématérialisation ou de conservation, incluant la gestion de la sécurité, notamment vis-à-vis du respect des propriétés de sécurité applicable à ces activités : Confidentialité, Intégrité, Disponibilité, Authenticité, Fiabilité, et Exploitabilité.

Les processus de dématérialisation ou de conservation peuvent inclure :

- la collecte de documents ;
- la préparation et numérisation de documents, incluant les configurations de numérisation minimales attendues ;
- la restitution, conservation ou suppression d'originaux ;
- la restitution, conservation ou suppression de copie à valeur probante ;
- la production et restitution d'attestation de valeur probante ;
- le traitement d'incident, notamment des incidents impactant la valeur probante d'un document ;
- les conditions d'accès au système de dématérialisation ou de conservation ;
- la gestion des rapports d'activités des opérateurs ;

- la continuité des activités et la gestion des désastres ;
- la modification du processus.

Annexe C
(informative)

Informations supplémentaires sur la dématérialisation

Avant la dématérialisation, chaque périphérique de dématérialisation de documents papier devrait être documenté avec :

a. les nombres minimum et maximum de couleurs et les niveaux de gris ;

b. les nombres minimum et maximum de dpi, de bits par pixel – un minimum de 200 est considéré comme un minimum pour obtenir un document numérisé représentatif ;

c. la possibilité de dématérialisation recto/verso ou uniquement recto ;

d. les différents formats à l'entrée, comme A3, A4 et A5 ;

e. les méthodes de correction d'images, comme le redressement, la suppression de points isolés, et la suppression des marges ;

f. les méthodes de compression des images,

g. le nombre de documents analogiques ou nombre de pages composant les documents analogiques pouvant être numérisés dans un laps de temps donné.

Pour répondre à la clause « 8.43 Mécanismes pour la dématérialisation » du chapitre 7, voici un exemple de preuves qui peuvent être collectées pour chacune des recommandations :

Recommandation	**Preuve associée**
La vérification de la complétude de l'opération de numérisation ;	Compter les pages d'une manière automatique. Par exemple en utilisant la fonction de comptage intégrée dans le scanneur.
La vérification de l'intégrité des documents numérisés ;	Hachage avant stockage dans le système de versement au client ou dans le système de gestion électronique de documents de production (si la conservation fait partie du périmètre du système) Hachage des documents numérisés en cours de stockage Comparaison des valeurs de hachage
Le stockage des informations spécifiques à chaque lot numérisé ;	Structure de données dans le système de gestion électronique de documents de production, avec notamment : • Identifiant de l'opérateur • Horodatage début et fin de l'opération de numérisation d'un lot • Nom du lot, nombre de documents, nombre de pages/document
Le stockage des informations de chaque document numérisé en termes d'horodatage, d'information sur les DPI, la couleur, le format, la taille ;	Structure de données dans le système de gestion électronique de documents de production, avec notamment : • Horodatage de l'opération de numérisation

	• DPI (200, 300, …) • Couleur (Noir et blanc, Niveaux de gris, Couleur) • Format (TIFF, PDF, …) • Taille (A3, A4, …)
Le contrôle qualité des documents numérisés, en suivant par exemple la norme ISO 2859 ;	Résultat de l'échantillonnage
Les opérations de conversion de format ;	Contrôle des valeurs de hachage avant conversion Nouvel hachage après conversion
L'adjonction des métadonnées aux documents numérisés et lots.	Vérification de l'existence des métadonnées

Bibliographie

[1] ISO/CEI 27001:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

[2] ISO/CEI 27002:2022, Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

[3] ISO 14641:2018, Archivage électronique — Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques — Spécifications