NORME INTERNATIONALE

**ISO/IEC 27040**

Première édition
2015-01-15

# Technologie de l'information — Techniques de sécurité — Sécurité de stockage

*Information technology — Security techniques — Storage security*

Numéro de référence
ISO/IEC 27040:2015(F)

© ISO/IEC 2015



## DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# Sommaire

Page

**Avant-propos** ..... **v**
**Introduction** ..... **vi**
**1 Domaine d'application** ..... **1**
**2 Références normatives** ..... **1**
**3 Termes et définitions** ..... **1**
**4 Symboles et abréviations** ..... **7**
**5 Vue d'ensemble et concepts** ..... **12**
5.1 Généralités ..... 12
5.2 Concepts relatifs au stockage ..... 12
5.3 Introduction à la sécurité du stockage ..... 13
5.4 Risques pour la sécurité du stockage ..... 15
5.4.1 Contexte ..... 15
5.4.2 Violations de données ..... 16
5.4.3 Corruption ou destruction de données ..... 17
5.4.4 Perte temporaire ou permanente d'accès/de disponibilité ..... 18
5.4.5 Défaillance à satisfaire les exigences légales, règlementaires ou juridiques ..... 18
**6 Prise en charge des contrôles** ..... **18**
6.1 Généralités ..... 18
6.2 Stockage à connexion directe (DAS) ..... 19
6.3 Réseau de stockage ..... 19
6.3.1 Contexte ..... 19
6.3.2 Réseaux de stockage (SAN) ..... 20
6.3.3 Stockage en réseau (NAS) ..... 24
6.4 Gestion du stockage ..... 26
6.4.1 Contexte ..... 26
6.4.2 Authentification et autorisation ..... 28
6.4.3 Sécurisation des interfaces de gestion ..... 29
6.4.4 Audit, redevabilité et surveillance de la sécurité ..... 30
6.4.5 Renforcement du système ..... 33
6.5 Stockage par blocs ..... 34
6.5.1 Stockage par Fibre Channel (FC) ..... 34
6.5.2 Stockage IP ..... 34
6.6 Stockage basé sur fichiers ..... 35
6.6.1 NAS sur NFS ..... 35
6.6.2 NAS sur SMB/CIFS ..... 36
6.6.3 NAS sur NFS parallèle ..... 37
6.7 Stockage basé sur les objets ..... 38
6.7.1 Stockage en nuage ..... 38
6.7.2 Dispositif de stockage basé sur les objets (OSD) ..... 39
6.7.3 Stockage associatif (CAS) ..... 40
6.8 Services de sécurité du stockage ..... 41
6.8.1 Nettoyage des données ..... 41
6.8.2 Confidentialité des données ..... 44
6.8.3 Réductions de données ..... 47
**7 Lignes directrices pour la conception et la mise en œuvre de la sécurité du stockage** ..... **47**
7.1 Généralités ..... 47
7.2 Principes de conception de la sécurité du stockage ..... 48
7.2.1 Défense en profondeur ..... 48
7.2.2 Domaines de sécurité ..... 49
7.2.3 Résilience de la conception ..... 50
7.2.4 Initialisation sécurisée ..... 50
7.3 Fiabilité, disponibilité et résilience des données ..... 50

© ISO/IEC 2015 – Tous droits réservés

7.3.1 Fiabilité ..... 50
7.3.2 Disponibilité ..... 51
7.3.3 Sauvegardes et réplication ..... 51
7.3.4 Reprise après sinistre et continuité des activités ..... 52
7.3.5 Résilience ..... 53
7.4 Conservation des données ..... 53
7.4.1 Conservation à long terme ..... 53
7.4.2 Conservation à court et moyen terme ..... 54
7.5 Confidentialité et intégrité des données ..... 55
7.6 Virtualisation ..... 58
7.6.1 Virtualisation du stockage ..... 58
7.6.2 Stockage pour les systèmes virtualisés ..... 59
7.7 Considérations sur la conception et la mise en œuvre ..... 60
7.7.1 Chiffrement et gestion des clés ..... 60
7.7.2 Alignement du stockage sur la politique ..... 61
7.7.3 Conformité ..... 61
7.7.4 Multilocation sécurisée ..... 63
7.7.5 Déplacement autonome sécurisé des données ..... 64

**Annexe A** (normative) **Nettoyage des supports** ..... **66**

**Annexe B** (informative) **Sélection des contrôles de sécurité du stockage appropriés** ..... **83**

**Annexe C** (informative) **Concepts de sécurité importants** ..... **106**

**Bibliographie** ..... **120**

 © ISO/IEC 2015 – Tous droits réservés

# Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/foreword.html.

Le comité responsable de ce document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

© ISO/IEC 2015 – Tous droits réservés

# Introduction

De nombreux organismes font face à la difficulté de la mise en œuvre de mesures de protection et de sécurité des données destinées à satisfaire à une large gamme d'exigences, dont la conformité légale et règlementaire. La sécurité associée aux systèmes et aux infrastructures de stockage est trop souvent défaillante en raison de mauvaises conceptions et d'un manque de familiarité avec les technologies de stockage ou, dans le cas des gestionnaires et administrateurs de stockage, d'une compréhension limitée des risques inhérents ou des concepts de base de la sécurité. Le résultat de cette situation est que les actifs numériques sont inutilement placés en situation de risque de compromission due à des violations de données, des corruptions volontaires, des prises d'otage ou d'autres évènements malveillants.

Le stockage de données a évolué dans un environnement où la sécurité était un problème secondaire, en raison de son historique de connectivité isolée, de technologies spécialisées et de la sécurité physique des centres de traitement de données. Même lorsque la connectivité du stockage a évolué pour utiliser des technologies telles que les protocoles TCP/IP, peu d'utilisateurs ont tiré parti des mécanismes de sécurité inhérents ou des mesures de sécurité recommandées.

La présente Norme internationale fournit des lignes directrices pour la sécurité du stockage dans les organismes. Elle prend en particulier en charge les exigences relatives aux systèmes de management de la sécurité de l'information (SMSI) conformément à l'ISO/IEC 27001. La présente Norme internationale recommande l'approche de gestion des risques liés à la sécurité de l'information telle que définie dans l'ISO/IEC 27005. L'organisme est responsable de la définition de son approche du management du risque, par exemple en fonction du domaine d'application du SMSI, du contexte de management du risque ou du secteur industriel. Un certain nombre de méthodologies existantes peuvent être utilisées dans le cadre décrit par la présente Norme internationale pour la mise en œuvre des exigences d'un SMSI.

La présente Norme internationale peut être utile aux gestionnaires et aux personnels concernés par la gestion des risques liés à la sécurité de l'information au sein d'un organisme et, le cas échéant, à des parties externes qui prennent en charge ces activités.

Les objectifs de la présente Norme internationale sont les suivants:

— attirer l'attention sur les risques;

— aider les organismes à mieux sécuriser leurs données stockées;

— donner une base pour l'audit, la conception et la revue des contrôles de sécurité du stockage.

Il est souligné que l'ISO/IEC 27040 donne des préconisations détaillées supplémentaires de mise en œuvre concernant les contrôles de sécurité du stockage qui sont décrits à un niveau normalisé de base dans l'ISO/IEC 27002.

Il convient de noter que la présente Norme internationale ne constitue pas un document normatif ou de référence pour les exigences de sécurité règlementaires et législatives. Bien qu'elle mette en exergue l'importance de ces influences, elle ne peut les déclarer spécifiquement puisqu'elles dépendent du pays, du type d'activités, etc.

 © ISO/IEC 2015 – Tous droits réservés

# Technologie de l'information — Techniques de sécurité — Sécurité de stockage

## 1 Domaine d'application

La présente Norme internationale donne des préconisations techniques détaillées concernant la manière dont les organismes peuvent définir un niveau approprié d'atténuation du risque grâce à l'emploi d'une approche reconnue et cohérente de la planification, la conception, la documentation et la mise en œuvre de la sécurité de stockage des données. La sécurité du stockage s'applique à la protection (la sécurité) des informations là où elles sont stockées et à la sécurité des informations transférées au moyen des liaisons de communication associées au stockage. La sécurité du stockage comprend la sécurité des dispositifs et des supports, la sécurité des activités de management associées aux dispositifs et aux supports, la sécurité des applications et des services et la sécurité relative aux utilisateurs finaux pendant la durée de vie de leurs dispositifs et supports et après la fin de leur utilisation.

La sécurité du stockage concerne toute personne impliquée dans la possession, l'exploitation ou l'utilisation de dispositifs, supports et réseaux de stockage de données. Il s'agit des cadres supérieurs, des acheteurs de produits et services de stockage et d'autres gestionnaires ou utilisateurs non techniciens, outre les gestionnaires et administrateurs ayant des responsabilités spécifiques en matière de sécurité de l'information ou de sécurité du stockage, d'exploitation du stockage, ou responsables du programme général de sécurité et du développement des politiques de sécurité de l'organisme. Elle concerne également toute personne impliquée dans la planification, la conception et la mise en œuvre des aspects architecturaux de la sécurité des réseaux de stockage.

La présente Norme internationale propose une description générale des concepts de sécurité du stockage et des définitions associées. Elle comprend des préconisations concernant les aspects relatifs aux menaces, à la conception et au contrôle ainsi que des scénarios de stockage et des technologies de stockage typiques. Elle donne de plus des références à d'autres Normes internationales et rapports techniques qui traitent des pratiques et techniques existantes pouvant être appliquées à la sécurité du stockage.

## 2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. 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).

UIT-T Y.3500 | ISO/IEC 17788:2014, *Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire*

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

ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

ISO/IEC 27005, *Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information*

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000, l'ISO/IEC 27005, ainsi que les suivants s'appliquent.

© ISO 2015 – Tous droits réservés

**3.1**
**bloc**
unité dans laquelle des données sont *stockées* (3.50) et récupérées sur des *dispositifs* à disque et à bande (3.14)

**3.2**
**effacer**
*nettoyer* (3.38) au moyen de techniques logiques les données dans tous les emplacements de stockage adressables pour la protection contre les techniques simples non invasives de récupération de données à l'aide de la même interface à la disposition de l'utilisateur

**3.3**
**compression**
processus de suppression des redondances dans les données numériques afin de réduire la quantité qu'il convient de *stocker* (3.50) ou de transmettre

[SOURCE: ISO/TR 12033:2009, 3.1]

Note 1 à l'article: Pour le *stockage* (3.43), une compression sans perte est requise (c'est-à-dire une compression utilisant une technique qui préserve le contenu complet des données originales et par laquelle les données originales peuvent être reconstruites avec exactitude).

**3.4**
**effacement cryptographique**
procédé de *nettoyage* (3.37) dans lequel la clé de chiffrement pour les *données cibles* chiffrées (3.52) est *nettoyée* (3.38), ce qui rend impossible la récupération des *données cibles* (3.52) chiffrées

**3.5**
**cryptopériode**
période déterminée au cours de laquelle l'utilisation d'une clé cryptographique spécifique est autorisée ou durant laquelle les clés cryptographiques d'un système donné sont effectives

[SOURCE: ISO 16609:2004, 3.9]

**3.6**
**données au repos**
données *stockées* (3.50) sur un *stockage non volatil* stable (3.30)

**3.7**
**violation de données**
compromission de sécurité qui entraîne la *destruction* (3.13) accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès à des données protégées transmises, *stockées* (3.50), ou soumises à un quelconque autre traitement

**3.8**
**données en mouvement**
données transférées d'un emplacement à un autre

Note 1 à l'article: Ces transferts impliquent généralement des interfaces accessibles et n'incluent pas les transferts internes (c'est-à-dire jamais exposés à l'extérieur d'une interface, d'une puce ou d'un dispositif).

**3.9**
**intégrité des données**
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[SOURCE: ISO 7498-2:1989, 3.3.21]


© ISO/IEC 2015 – Tous droits réservés

**3.10**
**déduplication**
procédé de réduction des besoins de *stockage* (3.43) par élimination des données redondantes, qui sont remplacées par un pointeur vers la copie de données unique

Note 1 à l'article: La déduplication est quelquefois considérée comme une forme de *compression* (3.3).

**3.11**
**démagnétiser**
rendre les données illisibles par l'application d'un fort champ magnétique au support

**3.12**
**détruire**
*nettoyer* (3.38) à l'aide de techniques qui rendent la récupération impossible au moyen de techniques de laboratoire de l'état de l'art et résultant en l'impossibilité d'utiliser le support pour le *stockage* (3.43) de données

Note 1 à l'article: *Désintégrer* (3.15), *incinérer* (3.21), *fondre* (3.25), *pulvériser* (3.34), et *broyer* (3.41) sont des formes de *nettoyage* par destruction (3.37).

**3.13**
**destruction**
résultat des actions entreprises pour assurer que le support ne peut pas être réutilisé selon son usage prévu et que la récupération des informations est pratiquement impossible ou extrêmement coûteuse

**3.14**
**dispositif**
organe mécanique, électrique ou électronique ayant une fin spécifique

[SOURCE: ISO/IEC 14776-372:2011, 3.1.10]

**3.15**
**désintégrer**
*détruire* (3.12) en divisant le support en ses composants

**3.16**
**stockage électronique d'informations**
données ou informations de tous types et provenant de toutes sources dont l'existence temporelle est mise en évidence par leur *stockage* (3.50) dans ou sur un quelconque support électronique

Note 1 à l'article: Le stockage électronique d'informations (ESI) comprend les courriers électroniques, les notes, lettres, tableurs, bases de données, documents de bureau, présentations, classiques et sous d'autres formats électroniques courants sur un ordinateur. Les ESI comprennent également les *métadonnées* (3.26) associées au système, à l'application et au fichier, comme les horodatages, l'historique de révision, le type de fichier, etc.

Note 2 à l'article: Le support électronique, sans y être limité, peut prendre la forme de *dispositifs de stockage* (3.45) et d'*éléments de stockage* (3.47).

**3.17**
**Fibre Channel**
interconnexion d'E/S en série pouvant prendre en charge plusieurs protocoles, comprenant l'accès à un *stockage* (3.43) de système ouvert, l'accès à un *stockage* (3.43) central et la mise en réseau

Note 1 à l'article: La technologie Fibre Channel prend en charge les topologies point à point, en boucle arbitrée et commutée, avec une variété de liaisons cuivre et optique fonctionnant à des vitesses comprises entre 1 Gbit/s et plus de 10 Gbit/s.

**3.18**
**protocole Fibre Channel**
protocole de transport série Small Computer System Interface (SCSI) utilisé sur les interconnexions *Fibre Channel* (3.17)

© ISO/IEC 2015 – Tous droits réservés

**3.19**
**passerelle**
*dispositif* (3.14) qui convertit un protocole en un autre protocole

**3.20**
**dans la bande**
communication ou transmission qui se produit dans un procédé ou un canal de communication préalablement établi

Note 1 à l'article: Les communications ou les transmissions prennent souvent la forme d'un protocole séparé, tel qu'un protocole de management, sur le même support que le protocole de données principal.

**3.21**
**incinérer**
*détruire* (3.12) en brûlant un support jusqu'à réduire en cendres

**3.22**
**programme malveillant**
logiciel malveillant conçu spécifiquement pour endommager ou interrompre un système, en attaquant la confidentialité, l'intégrité ou la disponibilité

Note 1 à l'article: Les virus et les chevaux de Troie sont des exemples de programmes malveillants.

[SOURCE: ISO/IEC 27033-1:2009, 3.22]

**3.23**
**temps moyen entre défaillances**
temps prévu entre des défaillances consécutives d'un système ou d'un composant

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1713, modifié — Le terme est mis en majuscules.]

**3.24**
**délai moyen de réparation**
durée prévue ou observée de retour d'un système ou d'un composant défaillant à un fonctionnement normal

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1714, modifié — Le terme est mis en majuscules.]

**3.25**
**fondre**
*détruire* (3.12) en faisant passer un support de l'état solide à l'état liquide, généralement par application de chaleur

**3.26**
**métadonnées**
données qui définissent et décrivent d'autres données

[SOURCE: ISO/IEC 11179-1:2004, 3.2.16]

**3.27**
**authentification multifactorielle**
authentification utilisant deux des facteurs suivants au moins:

— facteur de connaissance, «chose qu'une personne connaît»;

— facteur de possession, «chose qu'une personne possède»;

— facteur biométrique, «chose qu'une personne est ou est capable de faire».

[SOURCE: ISO 19092:2008, 4.42]


© ISO/IEC 2015 – Tous droits réservés

**3.28**
**multilocation**
attribution de ressources physiques ou virtuelles de sorte que plusieurs locataires et leurs calculs et données soient isolés et inaccessibles les uns aux autres

[SOURCE: Recommandation UIT-T Y.3500 | ISO/IEC 17788:2014, 3.2.27]

**3.29**
**stockage en réseau**
*dispositif de stockage* (3.45) ou système qui se connecte à un réseau et fournit des services d'accès aux fichiers à des systèmes informatiques

**3.30**
**stockage non volatil**
*stockage* (3.43) qui conserve son contenu après que l'alimentation est coupée

**3.31**
**hors bande**
communication ou transmission qui se produit à l'extérieur d'un procédé ou d'un canal de communication préalablement établi

**3.32**
**surdimensionnement**
technique utilisée par les *éléments de stockage* (3.47) et les *dispositifs de stockage* (3.45) par laquelle un sous-ensemble des supports disponibles est exposé par le biais de l'interface

Note 1 à l'article: Le *support de stockage* (3.48) est utilisé en interne et indépendamment par l'*élément de stockage* (3.47) pour améliorer la performance, l'endurance ou la fiabilité.

**3.33**
**point de chiffrement**
lieu de l'infrastructure de technologies de l'information et de la communication (TIC) où les données sont chiffrées en chemin vers leur *stockage* (3.43) et à l'inverse, où les données sont déchiffrées lorsqu'elles sont accédées depuis le *stockage* (3.43)

Note 1 à l'article: Le point de chiffrement n'est applicable qu'aux *données au repos* (3.6).

**3.34**
**pulvériser**
*détruire* (3.12) en broyant le support en poudre ou en poussière

**3.35**
**purger**
*nettoyer* (3.38) à l'aide de techniques physiques qui rendent la récupération impossible par des techniques de laboratoire de l'état de l'art, mais qui conservent le *support de stockage* (3.48) dans un état potentiellement réutilisable

**3.36**
**fiabilité**
capacité d'un système ou d'un composant à exécuter ses fonctions requises dans les conditions déclarées pendant une période spécifique

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2467, modifié — La seconde définition de l'ISO/IEC 9126-1:2001 et la mention «Voir...» ne sont pas incluses.]

**3.37**
**nettoyage**
processus ou méthode permettant de *nettoyer* (3.38)

© ISO/IEC 2015 – Tous droits réservés

**3.38**
**nettoyer**
rendre l'accès à des *données cibles* (3.52) sur un *support de stockage* (3.48) impossible à un niveau d'effort donné

Note 1 à l'article: *Effacer* (3.2), *purger* (3.35) et *détruire* (3.12) sont des actions pouvant être entreprises pour *nettoyer (3.38)* les *supports de stockage* (3.48).

**3.39**
**multilocation sécurisée**
type de *multilocation* (3.28) qui emploie des contrôles de sécurité pour une protection explicite contre les *violations de données* (3.7) et qui produit la validation de ces contrôles pour une bonne gouvernance

Note 1 à l'article: La multilocation sécurisée existe lorsque le profil de risque d'un locataire individuel n'est pas plus important qu'il ne le serait dans un environnement dédié à un seul locataire.

Note 2 à l'article: Dans les environnements très sécurisés, même l'identité des locataires est tenue secrète.

**3.40**
**force de la sécurité**
nombre associé à la quantité de travail requise pour casser un algorithme cryptographique ou un système

**3.41**
**broyer**
*détruire* (3.12) en découpant ou en déchirant un support en petites particules

**3.42**
**point de défaillance unique**
élément ou composant d'un système, trajet dans un système ou système tel que, s'il subit une défaillance, le système tout entier ou un réseau de systèmes sont incapables d'exécuter leurs fonctions primaires

Note 1 à l'article: un point de défaillance unique est souvent considéré comme un défaut de conception associé à un élément critique.

**3.43**
**stockage**
*dispositif* (3.14), fonction ou service prenant en charge l'entrée et la récupération de données

**3.44**
**réseau de stockage**
réseau dont le but principal est le transfert de données entre les systèmes informatiques et les *dispositifs de stockage* (3.45) et entre les *dispositifs de stockage* (3.45)

Note 1 à l'article: un SAN est constitué d'une infrastructure de communication, qui fournit les connexions physiques, et d'une couche de gestion, qui organise les connexions, les *dispositifs de stockage* (3.45) et les systèmes informatiques de sorte que le transfert de données soit sécurisé et robuste.

**3.45**
**dispositif de stockage**
tout *élément de stockage* (3.48) ou agrégation d'*éléments de stockage* (3.47), conçu(e) et construit(e) principalement à des fins de *stockage* (3.43) et de livraison de données

**3.46**
**écosystème de stockage**
système complexe de composants interdépendants qui fonctionnent ensemble pour activer des services et des capacités de *stockage* (3.43)

Note 1 à l'article: Les composants comprennent souvent des *dispositifs de stockage* (3.45), des éléments de stockage (3.47), des réseaux de stockage, une gestion du stockage et d'autres infrastructures de technologies de l'information et de la communication (TIC).

 © ISO/IEC 2015 – Tous droits réservés

**3.47**
**élément de stockage**
composant utilisé pour construire des *dispositifs de stockage* (3.45) et qui contribue au *stockage* (3.43) et à la livraison de données

Note 1 à l'article: Le lecteur de disque ou le lecteur de bande sont des exemples connus d'éléments de stockage.

**3.48**
**support de stockage**
**supports de stockage**
matériau sur lequel un *stockage électronique d'informations* (3.16) ou des données numériques sont ou peuvent être enregistrés

**3.49**
**sécurité du stockage**
application de contrôles physiques, techniques et administratifs permettant de protéger les systèmes et les infrastructures de stockage ainsi que les données *stockées* (3.50) à l'intérieur

Note 1 à l'article: La sécurité du stockage est dédiée à la protection des données (et des infrastructures de stockage) contre la divulgation, la modification ou la destruction non autorisées tout en garantissant leur disponibilité aux utilisateurs autorisés.

Note 2 à l'article: Ces contrôles peuvent être préventifs, de détection, correctifs, dissuasifs, de récupération ou de compensation.

**3.50**
**stocker**
enregistrer des données sur un *stockage volatil* (3.53) ou un *stockage non volatil* (3.30)

**3.51**
**authentification forte**
authentification au moyen de justificatifs cryptographiques

[SOURCE: ISO/TS 22600-1:2006, 2.23]

**3.52**
**données cibles**
informations soumises à un processus donné, comprenant généralement la plupart ou la totalité des informations sur une partie d'un *support de stockage* (3.48)

**3.53**
**stockage volatil**
*stockage* (3.43) qui échoue à conserver son contenu lorsque l'alimentation est coupée

**3.54**
**clé faible**
clé qui interagit avec un certain aspect de la définition d'un chiffre particulier afin d'affaiblir la *force de la sécurité* (3.40) du chiffre

## 4 Symboles et abréviations

| | |
|---|---|
| ACE | Entrée de contrôle d'accès (Access Control Entry) |
| ACL | Liste de contrôle d'accès (Access Control List) |
| AD | Active Directory |
| AES | Norme de chiffrement avancé (Advanced Encryption Standard) |
| ATA | Connexion AT (Advanced Technology Attachment) |

© ISO/IEC 2015 – Tous droits réservés