PROJET DE NORME INTERNATIONALE

ISO/IEC DIS 27002

ISO/IEC JTC **1**/SC **27** | Secrétariat: **DIN**

Début de vote:
2021-01-28

Vote clos le:
2021-04-22

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Information security, cybersecurity and privacy protection — Information security controls

ICS: 35.030

Numéro de référence
ISO/IEC DIS 27002:2021(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

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 attirée 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 ne saurait être tenue pour responsable 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 nature volontaire des normes, 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/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27002:2013 +Corr 1:2014 +Corr2:2015), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes :

— Le terme « Code de bonne pratique » a été retiré du titre du présent document pour mieux faire apparaître sa finalité, qui est de constituer un ensemble de référence pour les mesures de sécurité de l'information. Il ne s'agit pas d'un changement de finalité. La norme ISO/IEC 27002 a toujours eu pour but d'aider les organisations à s'assurer qu'aucune mesure nécessaire n'a été omise. Cette finalité est la même, quelle que soit l'utilisation prévue du présent document (voir l'Article 1). Nonobstant la présente déclaration, les recommandations données pour les différentes mesures individuelles reposent sur les meilleures pratiques reconnues au niveau international.

— L'objectif de constituer un ensemble de référence est réalisé en assurant la couverture exhaustive des différents modes de description des mesures de sécurité de l'information. Cela engendre de fait les recoupements et doublons dont il est fait mention en 0.3. C'est pourquoi la structure du document a été modifiée, de sorte à présenter les mesures à l'aide d'une taxinomie simple et des attributs correspondants.

— Certaines mesures ont été fusionnées, d'autres ont été supprimées, tandis que plusieurs nouvelles mesures ont été mises en place. La correspondance complète est indiquée à l'Annexe B.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

0 Introduction

0.1 Historique et contexte

Le présent document a pour objet de servir d'outil de référence permettant aux organisations de tous types et de toutes dimensions de déterminer et mettre en œuvre des mesures relatives au traitement du risque de sécurité de l'information dans un système de management de la sécurité de l'information (SMSI) basé sur l'ISO/IEC 27001. Il peut également être utilisé comme document d'orientation pour les organisations qui déterminent et mettent en œuvre les mesures de sécurité de l'information communément admises. Le présent document a également pour objet d'élaborer des lignes directrices de management de la sécurité de l'information spécifiques aux organisations et aux entreprises, en tenant compte de leur(s) environnement(s) particulier(s) de risques de sécurité de l'information. Des mesures organisationnelles ou spécifiques à l'environnement autres que celles qui figurent dans le présent document peuvent, si besoin, être déterminées par le biais d'une appréciation du risque afin de modifier le risque.

Des organisations de tous types et de toutes dimensions (recouvrant le secteur public et le secteur privé, à but lucratif ou non lucratif) créent, collectent, traitent, stockent et transmettent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, au cours de conversations et de présentations).

La valeur de l'information dépasse les mots, les chiffres et les images : la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles. Dans un monde interconnecté, les informations et les autres actifs associés, par exemple les intérêts commerciaux importants, méritent ou exigent une protection contre différentes sources de risques, aussi bien naturelles, qu'accidentelles ou délibérées.

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des politiques, des règles, des processus, des procédures, des structures organisationnelles et des fonctions matérielles et logicielles. Pour atteindre ses objectifs métier et de sécurité, il convient que l'organisation définisse, mette en œuvre, suive, révise et améliore ces mesures aussi souvent que nécessaire. Un système de management de la sécurité de l'information (SMSI) tel que celui spécifié dans l'ISO/IEC 27001 appréhende les risques de sécurité de l'information de l'organisation dans une vision globale et coordonnée, de manière à déterminer et mettre en œuvre un ensemble complet de mesures de sécurité de l'information dans le cadre général d'un système de management cohérent.

De nombreux systèmes d'information, notamment leur management et leurs opérations, n'ont pas été conçus dans un souci de sécurité au sens d'un système de management de la sécurité de l'information, tel que spécifié dans l'ISO/IEC 27001 et le présent document. Le niveau de sécurité qui ne peut être mis en œuvre que par des moyens techniques est limité et il convient de l'appuyer par des processus et activités de management adaptés. L'identification des mesures qu'il convient de mettre en place nécessite de procéder à une planification minutieuse et de prêter attention aux détails lors de la réalisation du traitement du risque.

Un système de management de la sécurité de l'information efficace requiert l'adhésion de tout le personnel de l'organisation. Il peut également nécessiter la participation d'autres parties intéressées, telles que des actionnaires ou des fournisseurs. Des conseils d'experts en la matière peuvent aussi s'avérer nécessaires.

Un système de management de la sécurité de l'information pertinent, adéquat et efficace procure l'assurance aux dirigeants de l'organisation et autres parties intéressées que leurs informations et les autres actifs associés sont conservés dans des conditions de sécurité satisfaisantes et protégés contre les menaces et dommages, ce qui permet à l'organisation d'atteindre les objectifs métier donnés.

0.2 Exigences de sécurité de l'information

Une organisation doit impérativement déterminer ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales :

a) l'appréciation du risque propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux. Cela peut être facilité ou appuyé par une appréciation du risque lié à la sécurité de l'information. Il convient ensuite de déterminer les mesures nécessaires de sorte que les risques résiduels pour l'organisation correspondent à ses critères d'acceptation des risques ;

b) les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses parties intéressées (partenaires commerciaux, prestataires de services, etc.) doivent répondre ainsi que leur environnement socioculturel ;

c) l'ensemble de principes, d'objectifs et d'exigences métier pour toutes les étapes du cycle de vie de l'information que l'organisation a élaborées pour mener à bien ses activités.

NOTE L'ISO/IEC 27005[11] fournit des recommandations relatives à la gestion des risques liés à la sécurité de l'information, comprenant des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation des risques, la communication relative aux risques, la surveillance des risques et la revue des risques.

0.3 Mesures

Une mesure est une action destinée à modifier ou à gérer un risque. Certaines des mesures indiquées dans le présent document sont des mesures destinées à modifier un risque, tandis que d'autres sont destinées à le gérer. Une politique de sécurité de l'information, par exemple, permet seulement de gérer le risque, tandis que la conformité à la politique de sécurité de l'information permet de modifier le risque. En outre, certaines mesures décrivent la même mesure générique dans plusieurs contextes de risque. Le présent document propose une combinaison générique de mesures de sécurité de l'information organisationnelles, liées aux personnes, d'ordre physique et technologiques, reposant sur les meilleures pratiques reconnues au niveau international.

0.4 Détermination des mesures

La détermination des mesures dépend des décisions organisationnelles consécutives à une appréciation du risque, avec un périmètre clairement défini. Il convient de baser les décisions relatives aux risques identifiés sur les critères d'acceptation des risques, les options de traitement des risques et la démarche de gestion des risques, appliqués par l'organisation. Il convient également que la détermination des mesures soit soumise à l'ensemble des lois et réglementations nationales et internationales applicables. La détermination des mesures de sécurité dépend également de la manière dont les mesures interagissent les unes avec les autres pour assurer une défense en profondeur.

L'organisation peut concevoir les mesures, le cas échéant, ou bien les identifier à partir de n'importe quelle source. Lors de la spécification desdites mesures, il convient que les organisations examinent les ressources et investissements nécessaires pour mettre en œuvre et appliquer une mesure par rapport à la valeur ajoutée qui en découle. Voir l'ISO/IEC 27016 pour un traitement plus détaillé de cet aspect.

Il convient de trouver un équilibre entre les ressources déployées pour mettre en œuvre les mesures et le préjudice que des incidents de sécurité sont susceptibles d'entraîner pour l'activité en l'absence de telles mesures. Il est recommandé de s'appuyer sur les résultats d'une appréciation du risque pour définir les actions de gestion appropriées, les priorités en matière de gestion des risques liés à la sécurité de l'information, et mettre en œuvre les mesures identifiées comme nécessaires pour contrer ces risques.

Certaines mesures décrites dans le présent document peuvent être considérées comme des principes directeurs pour le management de la sécurité de l'information et être appliquées à la plupart des organisations. De plus amples informations sur la détermination des mesures et autres options de traitement du risque figurent dans l'ISO/IEC 27005.

0.5 Mise au point de lignes directrices propres à l'organisation

Le présent document peut servir de base pour la mise au point de lignes directrices propres à une organisation Toutes les mesures et recommandations du présent document peuvent ne pas être applicables à toutes les organisations. Par ailleurs, des mesures et des lignes directrices ne figurant pas dans le présent document peuvent s'avérer nécessaires pour répondre aux besoins spécifiques de l'organisation et traiter les risques identifiés. Lors de la rédaction de documents contenant des lignes directrices ou des mesures supplémentaires, il peut être utile d'intégrer des références croisées aux articles du présent document à des fins de référence ultérieure.

0.6 Examen du cycle de vie

L'information est soumise à un cycle de vie naturel, depuis sa création jusqu'à son élimination. La valeur des informations et les risques qui y sont liés peuvent varier au cours de leur cycle de vie (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise revêt une importance moindre après la publication des informations, mais l'intégrité demeure essentielle). Dans une certaine mesure, l'importance de la sécurité de l'information subsiste à tous les stades.

Les systèmes d'information et autres actifs pertinents pour la sécurité de l'information sont soumis à des cycles de vie durant lesquels ils sont pensés, caractérisés, conçus, mis au point, testés, mis en œuvre, utilisés, mis à jour et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit prise en compte à tous les stades. Les projets de développement de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion à l'organisation d'améliorer les mesures de sécurité tout en prenant en compte ses propres risques et les enseignements tirés des incidents.

0.7 Normes associées

Alors que le présent document propose des recommandations portant sur un vaste éventail de mesures de sécurité liées à l'information d'utilisation courante dans nombre d'organisations différentes, les autres documents de la famille ISO/IEC 27000 présentent des conseils complémentaires ou des exigences relatifs à d'autres aspects du processus de management de la sécurité de l'information dans son ensemble.

Se reporter à l'ISO/IEC 27000 pour une introduction générale aux systèmes de management de la sécurité de l'information et à la famille de documents. L'ISO/IEC 27000 fournit un glossaire, définissant la plupart des termes utilisés dans la famille de documents ISO/IEC 27000, et décrit le domaine d'application et les objectifs pour chaque élément de cette famille.

Il existe des normes ISO/IEC 27002 sectorielles qui comportent des mesures supplémentaires destinées à traiter des domaines définis, telles que l'ISO/IEC 27017 pour les services en nuage, l'ISO/IEC 27701 pour la confidentialité, l'ISO/IEC 27019 pour l'énergie, l'ISO/IEC 27011 pour les organismes de télécommunications et l'ISO 27799 pour la santé. Ces normes figurent dans la Bibliographie et certaines d'entre elles sont référencées dans les recommandations et autres sections d'information des Articles 5 à 8.

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

1 Domaine d'application

Le présent document fournit un ensemble de référence de mesures de sécurité de l'information génériques, accompagné de préconisations de mise en œuvre. Le présent document est conçu pour être utilisé par les organisations :

a) dans le contexte d'un système de management de la sécurité de l'information selon l'ISO/IEC 27001 ;

b) pour la mise en œuvre de mesures de sécurité de l'information selon les meilleures pratiques reconnues au niveau international ;

c) pour l'élaboration de leurs propres lignes directrices de management de la sécurité de l'information.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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).

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

3 Termes, définitions et abréviations

3.1 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes :

— ISO Online browsing platform : disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia : disponible à l'adresse http://www.electropedia.org/.

3.1.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès physique et logique aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier

3.1.2
actif
tout élément représentant de la valeur pour l'organisation

Note à l'article 1 : On peut distinguer deux types d'actifs liés à la sécurité de l'information :

- les actifs primordiaux :
  - processus et activités métier ;
  - informations ;
- les actifs en support (sur lesquels reposent les actifs primordiaux) de tous les types :
  - matériel ;
  - logiciel ;
  - réseau ;
  - personnel ;
  - site ;
  - structure de l'organisme.

3.1.3
attaque
tentative de détruire, de rendre public, de modifier ou toute tentative d'invalider, de voler, d'accéder à un actif sans autorisation ou de faire un usage non autorisé de celui-ci

3.1.4
authentification
moyen pour une *entité* (3.1.11) d'assurer la légitimité d'une caractéristique revendiquée

3.1.5
authenticité
propriété selon laquelle une *entité* (3.1.11) est ce qu'elle revendique être

3.1.6
chaîne de traçabilité
possession démontrable, déplacement, manipulation et emplacement de matériel d'un moment donné à un autre

Note 1 à l'article : La notion de matériel englobe les informations et les autres actifs associés dans le contexte de l'ISO/IEC 27002.

[SOURCE : ISO/IEC 27050-1:2019, 3.1, modifiée — Ajout d'une Note 1 à l'article]

3.1.7
informations confidentielles
informations qu'il convient de ne pas rendre disponibles ou divulguer à des personnes, des entités ou des processus non autorisés

3.1.8
mesure
action destinée à gérer et/ou modifier un risque

Note 1 à l'article : Les mesures englobent, sans toutefois s'y limiter, n'importe quel processus, politique, dispositif, pratique ou autres conditions et/ou actions destinées à gérer et/ou modifier un risque.

Note 2 à l'article : Les mesures n'aboutissent pas toujours nécessairement à la modification voulue ou supposée.

[SOURCE : ISO 31000:2018, 3.8, modifiée]

3.1.9
perturbation
incident, anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison de produits et à la fourniture de services prévues selon les objectifs d'une organisation

[SOURCE : ISO 22301:2019, 3.10]

3.1.10
terminal final
dispositif matériel TIC connecté au réseau

Note 1 à l'article : Un terminal final peut correspondre à un ordinateur de bureau, un ordinateur portable, un smartphone, une tablette, un client léger, une imprimante ou autre matériel spécialisé tel qu'un compteur intelligent ou un dispositif de l'Internet des Objets.

3.1.11
entité
élément pertinent aux fins de fonctionnement d'un domaine et qui possède une existence manifestement distincte

Note 1 à l'article : Une entité peut avoir une matérialisation physique ou logique.

EXEMPLE Une personne, une organisation, un dispositif, un groupe d'éléments de cette nature, un abonné humain à un service de télécommunications, une carte SIM, un passeport, une carte d'interface réseau, une application logicielle, un service ou un site Web.

[SOURCE : ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
moyen de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou le local les abritant

[SOURCE : ISO/IEC 27000:2018, 3.27, modifiée — « moyens » a été remplacé par « moyen »]

3.1.13
violation de sécurité de l'information
compromission de sécurité qui entraîne la destruction non intentionnelle, la perte, l'altération, la divulgation ou l'accès à des informations protégées transmises, stockées ou soumises à un quelconque autre traitement

3.1.14
événement lié à la sécurité de l'information
occurrence indiquant une possible *violation* (3.1.5) de la sécurité de l'information ou une violation des *mesures* (3.1.8)

[SOURCE : ISO/IEC 27035-1:2016, 3.3]

3.1.15
incident lié à la sécurité de l'information
un ou plusieurs *événements liés à la sécurité de l'information* (3.1.13), pouvant porter préjudice aux actifs d'une organisation ou compromettre son fonctionnement

[SOURCE : ISO/IEC 27035-1:2016, 3.4]

3.1.16
gestion des incidents liés à la sécurité de l'information
exercice d'une approche cohérente et efficace de la prise en charge des *incidents liés à la sécurité de l'information* (3.1.14)

[SOURCE : ISO/IEC 27035-1:2016, 3.5]

3.1.17
système d'information
ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information

[SOURCE : ISO/IEC 27000:2018, 3.35]

3.1.18
partie intéressée (terme privilégié)
partie prenante (terme toléré)
personne ou organisme susceptible d'affecter, d'être affecté ou de s'estimer affecté par une décision ou une activité

[SOURCE : ISO/IEC 27000:2018, 3.37]

3.1.19
non-répudiation
capacité à prouver l'occurrence d'un événement ou d'une action donné(e) et des *entités* (3.1.11) qui en sont à l'origine

3.1.20
personnel
nombre de personnes effectuant un travail sous le contrôle de l'organisation

Note 1 à l'article : Le concept de personnel englobe les membres de l'organisation, tels que l'organe de gouvernance, la direction, les employés, le personnel temporaire, les sous-traitants et les bénévoles.

3.1.21
données à caractère personnel
DCP
toute information qui (a) peut être utilisée pour établir un lien entre les informations et la personne physique à laquelle ces informations se rapportent, ou qui (b) est ou peut être directement ou indirectement associée à une personne physique

Note 1 à l'article : La « personne physique » référencée dans la définition est la personne concernée (3.1.22). Pour déterminer si une personne concernée est identifiable, il convient de tenir compte de tous les moyens pouvant être raisonnablement utilisés par la partie prenante du domaine de la vie privée qui détient les données, ou par toute autre partie, afin d'établir le lien entre l'ensemble de DCP et la personne physique.

[SOURCE : ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22
personne concernée
personne physique à qui se rapportent les *données à caractère personnel (DCP)* (3.1.20)

Note 1 à l'article : Selon la juridiction et la loi applicable en matière de protection des données et de la vie privée, le terme « sujet des données » peut également être employé en lieu et place de « personne concernée ».

[SOURCE : ISO/IEC 29100:2011, 2.11]

3.1.23
sous-traitant de DCP
partie prenante en matière de protection de la vie privée qui traite des données à caractère personnel (DCP) pour le compte d'un responsable de traitement de DCP et conformément à ses instructions

[SOURCE : ISO/IEC 29100:2011, 2.12]

3.1.24
politique
intentions et orientations d'un organisme, telles que formalisées par sa direction

[SOURCE : ISO/IEC 27000:2018, 3.53]

3.1.25
évaluation de l'impact sur la vie privée
PIA
processus global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des données à caractère personnel, dans le cadre plus large du système de management des risques d'une organisation

[SOURCE : ISO/IEC 29134:2017, 3.7, modifiée — Suppression de la note 1 à l'article]

3.1.26
procédure, mode opératoire
manière spécifiée de réaliser une activité ou un *processus* (3.1.25)

[SOURCE : ISO 30000:2009, 3.12, modifiée, « mode opératoire » a été ajouté]

3.1.27
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[SOURCE : ISO 9000:2005, 3.4.1]

3.1.28
enregistrement
informations créées, reçues et préservées comme preuve et actif par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite des opérations liées à son activité

Note 1 à l'article : Dans ce contexte, les obligations légales comprennent toutes les exigences légales, statutaires, réglementaires et contractuelles.

[SOURCE : ISO 15489-1:2016, modifiée — Ajout de la « note 1 à l'article »]

3.1.29
point de récupération des données
RPO
point à partir duquel les données doivent être restaurées après la survenue d'une *perturbation* (3.1.9)

[SOURCE : ISO/IEC 27031:2011, 3.12]

3.1.30
objectif de délai de reprise
RTO
période au cours de laquelle les niveaux de service minimaux et/ou les produits et les systèmes, applications ou fonctions qui en relèvent doivent être rétablis après la survenue d'une *perturbation* (3.1.9)

[SOURCE : ISO/IEC 27031:2011, 3.13]

3.1.31
fiabilité
propriété relative à un comportement et à des résultats prévus et cohérents

3.1.32
règle
principe admis ou instruction formulant les attentes de l'organisation sur ce qu'il convient de faire, ce qui est autorisé ou ce qui ne l'est pas

Note 1 à l'article : Les règles peuvent être exprimées de façon formelle dans des politiques ainsi que d'autres types de documents.

3.1.33
information sensible
information qu'il est nécessaire de protéger contre l'indisponibilité, l'accès non autorisé, la modification ou la divulgation publique en raison des effets négatifs possibles sur une personne, une organisation, la sécurité nationale ou la sécurité publique

3.1.34
menace
cause potentielle d'un incident indésirable, pouvant porter préjudice à un système ou à une organisation

[SOURCE : ISO/IEC 27000:2018, 3.74]

3.1.35
politique portant sur un thème
intention et orientation sur un sujet ou thème spécifique, telles qu'elles sont officiellement formulées par la hiérarchie

Note 1 à l'article : Une politique portant sur un thème peut exprimer de façon formelle des règles, des directives ou des normes d'organisation.

Note 2 à l'article : Certaines organisations utilisent d'autres termes pour désigner les politiques portant sur des thèmes.

Note 3 à l'article : Les politiques portant sur des thèmes auxquelles il est fait référence dans le présent document relèvent de la sécurité de l'information.

EXEMPLES Politique portant sur le thème du contrôle d'accès, politique portant sur le thème du bureau propre et de l'écran vide.

3.1.36
utilisateur
partie intéressée (3.1.17) ayant accès aux *systèmes d'information* (3.1.16) de l'organisation

EXEMPLE Personnel, clients, fournisseurs.

3.1.37
vulnérabilité
faille dans un actif ou dans une *mesure de sécurité* (3.1.8) qui peut être exploitée par une ou plusieurs *menaces* (3.1.32)

[SOURCE : ISO/IEC 27000:2018, 3.77]

3.2 Abréviations

BIA	bilan d'impact sur l'activité
BYOD	apportez votre équipement personnel de communication (AVEC) [*bring your own device*]
CCTV	système de vidéosurveillance en circuit fermé [*closed circuit television*]
DCP	données à caractère personnel
DNS	système de nom de domaine [*domain name system*]

GAB	guichet automatique de banque
GPS	système mondial de localisation [*global positioning system*]
IAM	gestion des identités et des accès [*identity and access management*]
IDE	environnement de développement intégré [*integrated development environment*]
IDS	système de détection des intrusions [*intrusion detection system*]
IP	protocole Internet [*Internet Protocol*]
IPS	système de prévention des intrusions [*intrusion prevention system*]
ISMS	système de management de la sécurité de l'information [*information security management system*]
IT	technologies de l'information [*information technology*]
NTP	protocole de synchronisation réseau [*network time protocol*]
PIA	évaluation de l'impact sur la vie privée [*privacy impact assessment*]
PIN	numéro d'identification personnel [*personal identification number*]
PKI	infrastructure de clé publique [*public key infrastructure*]
RH	ressources humaines
ROM	mémoire morte [*read only memory*]
RPO	point de récupération des données [*recovery point objective*]
RTO	objectif de délai de reprise [*recovery time objective*]
SD	numérique sécurisé [*secure digital*]
SIEM	gestion de l'information et des événements de sécurité [*security information and event management*]
SMS	service de messagerie courte [*short message service*]
SQL	langage de requêtes structuré [*structured query language*]
SSO	authentification unique [*single sign-on*]
TIC	Technologies de l'Information et de la Communication
UEBA	analyse comportementale des utilisateurs et des entités [*user and entity behaviour analytics*]
URL	localisateur uniforme de ressource [*uniform resource locator*]
USB	bus série universel [universal serial bus]
VM	machine virtuelle [*virtual machine*]
VPN	réseau privé virtuel [*virtual private network*]

4 Structure du présent document

4.1 Articles

Le présent document est structuré comme suit :

a) mesures organisationnelles (Article 5) ;

b) mesures liées aux personnes (Article 6) ;

c) mesures d'ordre physique (Article 7) ;

d) mesures technologiques (Article 8).

Il contient 2 annexes informatives :

— Annexe A – Utilisation des attributs

— Annexe B – Correspondance avec l'ISO/IEC 27002:2013

L'Annexe A explique la façon dont une organisation peut utiliser des attributs (voir 4.2) pour créer ses propres vues en fonction des attributs de mesure définis dans le présent document ou créés par ses soins.

L'Annexe B montre la correspondance entre les mesures figurant dans la présente édition de l'ISO/IEC 27002 et la précédente édition 2013.

4.2 Thèmes et attributs

Les mesures de sécurité données dans les Articles 5 à 8 sont catégorisées sous forme de *thèmes*.

Les différentes catégories de mesures de sécurité sont les suivantes :

a) personnes, si elles concernent des individus ;

b) physiques, si elles concernent des objets physiques ;

c) technologiques, si elles concernent la technologie ;

d) sinon, elles appartiennent à la catégorie organisationnelle.

L'organisation peut utiliser des attributs pour créer plusieurs *vues* représentant différentes catégorisations des mesures de sécurité, telles qu'envisagées d'un point de vue différent des thèmes. Les attributs peuvent être utilisés pour filtrer, trier ou présenter les mesures dans plusieurs vues destinées à différents publics. L'Annexe A explique comment il est possible d'y parvenir et fournit un exemple de *vue*.

À titre d'exemple, chaque mesure indiquée dans le présent document a été associée à quatre *attributs* avec les *valeurs d'attributs* correspondantes (précédées par le signe « # » pour en faciliter la recherche), de la façon suivante :

a) types de mesures de sécurité (#Prévention, #Détection, #Correction) ;

Le type de mesure de sécurité est un attribut qui permet d'appréhender une mesure du point de vue du moment et de la façon dont cette mesure impacte le niveau du risque en cas de survenue d'un incident lié à la sécurité de l'information. Les valeurs d'attributs correspondent à #Prévention (la mesure agit avant qu'une menace ne survienne), #Détection (la mesure agit lorsqu'une menace survient) et #Correction (la mesure agit après la survenue d'une menace).

b) propriétés de sécurité de l'information (#Confidentialité, #Intégrité, #Disponibilité) ;

Les propriétés de sécurité de l'information sont un attribut qui permet d'appréhender les mesures du point de vue de la caractéristique de l'information que la mesure contribuera à préserver. Les valeurs d'attributs correspondent à #Confidentialité, #Intégrité et #Disponibilité.

c) concepts de cybersécurité (#Identification, #Protection, #Détection, #Traitement, #Récupération) ;

Les concepts de cybersécurité sont un attribut qui permet d'appréhender les mesures de sécurité du point de vue de leur association aux concepts de cybersécurité tels que définis dans le cadre de cybersécurité décrit dans l'ISO/IEC TS 27101. Les valeurs d'attributs correspondent à #Identification, #Protection, #Détection, #Traitement et #Récupération.

d) capacités opérationnelles ;

Les capacités opérationnelles sont un attribut qui permet d'appréhender les mesures du point de vue du praticien par rapport aux capacités de sécurité de l'information. Les valeurs d'attributs correspondent à #Gouvernance, #Gestion_des_actifs, #Protection_des_informations, #Sécurité_des_ressources_humaines, #Sécurité_physique, #Sécurité_système_et_réseau, #Sécurité_des_applications, #Configuration_sécurisée, #Gestion_des_identités_et_des_accès, #Gestion_des_menaces_et_des_vulnérabilités, #Continuité, #Sécurité_des_relations_fournisseurs, #Législation_et_conformité, #Gestion_des_événements_de_sécurité_de_l'information et #Assurance_de_sécurité_de_l'information.

e) domaines de sécurité (#Gouvernance_et_écosystème, #Protection, #Défense, #Résilience) ;

Les domaines de sécurité sont un attribut qui permet d'appréhender les mesures du point de vue des domaines, de l'expertise, des services et des produits relatifs à la sécurité de l'information. Les valeurs d'attributs correspondent à #Gouvernance_et_écosystème, #Protection, #Défense et #Résilience.

Les attributs donnés dans le présent document sont sélectionnés parce qu'ils sont considérés comme suffisamment génériques pour être utilisés par différents types d'organisations et que les valeurs d'attributs correspondantes sont indépendantes de l'organisation. Les organisations peuvent choisir d'écarter un ou plusieurs des attributs donnés dans le présent document. Elles peuvent également créer elles-mêmes des attributs (avec les valeurs d'attributs correspondantes) de sorte à définir leurs propres vues organisationnelles. Le Tableau A.2 comprend des exemples de tels attributs.

4.3 Disposition des mesures

Chaque mesure de sécurité se présente comme suit :

— **titre de la mesure :** nom court de la mesure ;

— **tableau d'attributs** : tableau indiquant la ou les valeurs de chaque attribut pour la mesure concernée ;

— **mesure de sécurité :** description de la mesure ;

— **objet** : texte expliquant l'objet de la mesure ;

— **préconisations :** préconisations de mise en œuvre de la mesure ;

— **autres informations :** texte explicatif ou références aux autres documents connexes.

Des sous-titres sont utilisés dans le texte des préconisations relatives à certaines mesures par souci de lisibilité. Ce principe est appliqué lorsque les préconisations sont longues et portent sur plusieurs sujets. Des titres de ce type ne sont pas nécessairement utilisés dans le texte de toutes les préconisations. Le sous-titre est indiqué en tant que Sous-titre.

5 Mesures organisationnelles

5.1 Politiques de sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Résilience

Mesure de sécurité

Il convient de définir une politique de sécurité de l'information et des politiques portant sur des thèmes, de les faire approuver par la direction, de les publier, de les communiquer et d'en demander confirmation au personnel et aux parties intéressées concernés, ainsi que de les réviser à intervalles planifiés et si des changements notoires interviennent.

Objectif

Assurer l'applicabilité dans le temps, l'adéquation, l'efficacité des orientations de la direction et le soutien de la sécurité de l'information en accord avec les exigences liées à l'activité et les exigences légales, statutaires, réglementaires et contractuelles.

Préconisations

Il convient que les organisations définissent, à leur plus haut niveau, une « politique de sécurité de l'information », qui soit approuvée par la direction et qui décrive l'approche adoptée par l'organisation pour gérer la sécurité de ses informations.

Il convient que la politique de sécurité de l'information réponde à des exigences dérivées des éléments suivants :

a) stratégie et exigences de l'entreprise ;

b) réglementations, législation et contrats ;

c) environnement réel et anticipé des menaces liées à la sécurité de l'information.

Il convient que cette politique de sécurité de l'information comporte des précisions concernant :

d) la définition de la sécurité de l'information ;

e) les objectifs de sécurité de l'information ou le cadre pour l'établissement de ces objectifs ;

f) les principes devant guider toutes les activités liées à la sécurité de l'information ;

g) l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information ;

h) l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information ;

i) l'attribution de responsabilités en matière de management de la sécurité de l'information à des fonctions définies ;

j) des procédures de traitement des dérogations et des exceptions.

Il convient que la direction approuve tout changement apporté à la politique de sécurité de l'information.

Il convient qu'à un niveau inférieur, la politique de sécurité de l'information soit étayée par des politiques portant sur des thèmes, qui imposent en outre la mise en œuvre de mesures de sécurité de l'information. Les politiques portant sur des thèmes sont de manière générale structurées pour répondre aux besoins de certains groupes cibles d'une organisation ou pour englober certains domaines de la sécurité. Il convient que les politiques de ce type soient en adéquation avec la politique de sécurité de l'information de l'organisation et qu'elles en soient complémentaires.

Voici des exemples de thèmes :

a) le contrôle d'accès ;

b) la sécurité physique et environnementale ;

c) la gestion des actifs ;

d) le transfert de l'information ;

e) la sécurité des réseaux ;

f) la gestion des incidents liés à la sécurité de l'information ;

g) la sauvegarde ;

h) la cryptographie et la gestion des clés ;

i) la classification et la gestion de l'information ;

j) la gestion des vulnérabilités techniques ;

k) le développement sécurisé.

Il convient que les politiques portant sur des thèmes soient approuvées par les dirigeants concernés.

Il convient que les politiques portant sur des thèmes soient communiquées au personnel et aux parties intéressées extérieures concernés, sous une forme pertinente, accessible et compréhensible par leurs destinataires. L'organisation peut déterminer les formats et les noms de ces documents de politique en fonction de ses besoins. Dans certaines organisations, la politique de sécurité de l'information et les politiques portant sur des thèmes peuvent figurer dans un seul et unique document. L'organisation peut désigner ces politiques portant sur des thèmes comme des normes, des directives, des politiques ou autres.

Il convient d'attribuer la responsabilité du développement, de la revue et de l'approbation des politiques portant sur des thèmes au personnel pertinent en fonction de son niveau d'autorité et de sa compétence technique. Il convient que la revue comporte une appréciation des possibilités d'amélioration des politiques de l'organisation et du management de la sécurité de l'information pour répondre aux changements intervenant dans :

a) la stratégie commerciale de l'organisation ;

b) l'environnement technique de l'organisation ;

c) les réglementations, la législation et les contrats ;

d) les risques liés à la sécurité de l'information ;

e) l'environnement réel et anticipé des menaces liées à la sécurité de l'information ;

f) les enseignements tirés des événements et incidents liés à la sécurité de l'information.

Il convient que la revue des politiques de sécurité de l'information tienne compte des résultats des revues et audits de management.

Si l'une quelconque des politiques de sécurité de l'information est diffusée hors de l'organisation, il convient de veiller à ne pas divulguer d'informations confidentielles.

Le Tableau 1 illustre les différences entre politique de sécurité de l'information et politique portant sur un thème.

Tableau 1 — Différences entre politique de sécurité de l'information et politique portant sur un thème

	Général/Haut niveau	**Spécifique/Détaillé**
Approbation et documentation formelles	Politique de sécurité de l'information (3.1.22) Approuvée par la direction générale	Politique portant sur un thème (3.1.33) Approuvée par le niveau de direction approprié

Informations supplémentaires

Les politiques de sécurité de l'information portant sur des thèmes peuvent différer d'une organisation à l'autre.

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

Type de mesure de sécurité	**Propriétés de sécurité de l'information**	**Concepts de cybersécurité**	**Capacités opérationnelles**	**Domaines de sécurité**
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Protection #Résilience

Mesure de sécurité

Il convient de définir et d'attribuer les fonctions et responsabilités liées à la sécurité de l'information selon les besoins de l'organisation.

Objectif

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

Préconisations

Il convient d'attribuer les fonctions et responsabilités en matière de sécurité de l'information conformément à la politique de sécurité de l'information et aux politiques portant sur des thèmes (voir 5.1). Il convient de déterminer les responsabilités en ce qui concerne la protection des actifs individuels et la mise en œuvre de processus de sécurité spécifiques. Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et, en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de recommandations détaillées, appropriées à certains sites et moyens de traitement de l'information. Il convient de déterminer les responsabilités du site du point de vue de la protection des actifs et de la mise en œuvre des processus de sécurité spécifiques.

Il convient de déterminer les responsabilités de toutes les personnes qui utilisent les informations et les systèmes d'information d'une organisation. Les personnes auxquelles ont été attribuées des responsabilités en matière de sécurité de l'information peuvent affecter des tâches de sécurité à des tiers. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée.

Il convient de définir, de documenter et de communiquer chaque domaine de sécurité dont des personnes sont responsables. Il convient de définir et de documenter les différents niveaux d'autorisation. Il convient que les personnes qui occupent une fonction liée à la sécurité de l'information maîtrisent les connaissances et possèdent les aptitudes qu'exige la fonction. Il convient de les aider à se tenir au courant des évolutions associées à la fonction, qui s'avèrent nécessaires pour en assumer les responsabilités.

Informations supplémentaires

De nombreuses organisations désignent un responsable de la sécurité de l'information pour assumer la responsabilité d'ensemble de l'élaboration et de la mise en œuvre de la politique de sécurité de l'information et pour corroborer l'identification des risques et des mesures d'atténuation correspondantes.

Cependant, la mise en place des ressources et des mesures reste bien souvent l'affaire des autres managers. Une pratique courante consiste à nommer, pour chaque actif, un propriétaire qui devient alors responsable de la protection quotidienne de cet actif.

Selon la taille de l'organisation et les ressources dont elle dispose, la sécurité de l'information peut être assurée par une fonction dédiée ou constituer une tâche réalisée en plus d'une fonction existante.

5.3 Séparation des tâches

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gouvernance	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de séparer les tâches et domaines de responsabilité incompatibles.

Objectif

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

Préconisations

La séparation des tâches et des domaines de sécurité vise à séparer les tâches incompatibles entre plusieurs personnes pour éviter qu'une personne donnée ne soit elle-même amenée à réaliser des tâches potentiellement incompatibles. Il convient de séparer le déclenchement d'un événement de son autorisation. Dans certains contextes, il convient également de séparer les tâches à haut risque.

Il convient que l'organisation détermine les tâches et domaines de responsabilité à séparer. Les activités suivantes peuvent, par exemple, nécessiter une séparation :

a) lancement, approbation et exécution d'un changement ;

b) demande, approbation et mise en œuvre de droits d'accès ;

c) conception, mise en œuvre et revue de code ;

d) développement de logiciel et administration du système de production ;

e) utilisation et administration d'applications ;

f) utilisation d'applications et administration de bases de données ;

g) conception, audit et garantie des mesures de sécurité de l'information.

Il convient d'envisager la possibilité de collusion lors de la conception des mesures de séparation. Les organisations de petite taille peuvent avoir des difficultés à réaliser une séparation des tâches, mais il convient d'appliquer ce principe dans la mesure du possible. Lorsqu'il est difficile de procéder à la séparation des tâches, il convient d'envisager d'autres mesures comme la surveillance des activités, des systèmes de traçabilité et la supervision de la direction.

En cas d'utilisation de systèmes de contrôle d'accès basés sur les rôles, il convient de veiller à ne pas attribuer de fonctions incompatibles aux personnes. En présence d'un nombre élevé de fonctions, il convient que les organisations envisagent de se doter d'outils automatiques pour identifier les conflits et faciliter leur élimination. Il convient de définir et d'attribuer les rôles avec soin pour réduire au minimum les problèmes d'accès si une fonction est supprimée ou réattribuée.

Informations supplémentaires

Aucune autre information.

5.4 Responsabilités de la direction

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient que la direction représente un modèle de fonction en termes de sécurité de l'information et qu'elle amène tout le personnel à appliquer les mesures de sécurité de l'information conformément à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux procédures établies de l'organisation.

Objectif

Faire en sorte que la direction comprenne son rôle en matière de sécurité de l'information et qu'elle prenne des mesures visant à s'assurer que tout le personnel soit sensibilisé aux responsabilités liées à la sécurité de l'information et qu'il assume ces responsabilités.

Préconisations

Il convient que la direction manifeste son soutien à la politique de sécurité de l'information, aux politiques portant sur des thèmes, aux procédures et aux mesures de sécurité de l'information.

Il convient qu'il relève des responsabilités de la direction de s'assurer que le personnel :

a) soit correctement informé sur ses fonctions et ses responsabilités en matière de sécurité de l'information avant de se voir accorder l'accès à l'information ou aux systèmes d'information de l'organisation ;

b) prenne connaissance des lignes directrices spécifiant les attentes en matière de sécurité de l'information qu'impliquent ses fonctions au sein de l'organisation ;

c) se voie confier la mission d'appliquer la politique de sécurité de l'information et les politiques portant sur des thèmes de l'organisation ;

d) acquière un niveau de sensibilisation à la sécurité de l'information en adéquation avec ses fonctions et responsabilités au sein de l'organisation (voir 6.3) ;

e) respecte les conditions de son embauche, de son contrat de travail ou de son engagement, ce qui inclut notamment la politique de sécurité de l'information de l'organisation et les méthodes de travail appropriées ;

f) dispose en permanence des compétences et qualifications de sécurité de l'information appropriées grâce à une formation professionnelle permanente ;

g) lorsque cela s'avère possible, se voie proposer un canal confidentiel pour signaler les violations de la politique de sécurité de l'information, des politiques portant sur des thèmes ou des procédures de sécurité de l'information (« dénonciation »). Cela peut permettre d'effectuer des signalements anonymes ou de prendre des dispositions visant à garantir que l'identité de la personne qui signale la violation soit uniquement connue des personnes qui ont à gérer ces types de signalements ;

h) reçoive les ressources adéquates et bénéficie du temps de planification de projet nécessaire à la mise en œuvre des processus et mesures de sécurité de l'organisation.

Informations supplémentaires

Si rien n'est entrepris pour sensibiliser le personnel quant à ses responsabilités en matière de sécurité de l'information, ce dernier peut causer des préjudices considérables à l'organisation.

5.5 Relations avec les autorités

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense #Résilience

Mesure de sécurité

Il convient que l'organisation établisse et entretienne des relations avec les autorités compétentes.

Objectif

Assurer la bonne circulation de l'information à l'égard de la sécurité, entre l'organisation et les autorités légales, réglementaires et de surveillance compétentes.

Préconisations

Il convient que l'organisation spécifie quand et comment il convient de contacter les autorités compétentes (par exemple, les autorités chargées de l'application des lois, les organismes de réglementation, les autorités de surveillance) et la façon dont il convient de signaler dans les meilleurs délais les incidents liés à la sécurité de l'information.

Il convient de s'appuyer également sur les relations avec les autorités pour faciliter la compréhension des attentes actuelles et futures desdites autorités, concernant par exemple les réglementations applicables en matière de sécurité de l'information.

Informations supplémentaires

Les organisations subissant une attaque peuvent recourir aux autorités pour engager des actions à l'encontre de la source de l'attaque.

Entretenir de telles relations peut constituer une exigence afin de favoriser la gestion des incidents (voir 5.24 à 5.28) ou le processus de planification de la continuité d'activité et des mesures d'urgence (voir 5.29 et 5.30). Les relations avec les autorités de régulation sont également utiles pour anticiper et préparer les changements à venir sur le plan juridique ou réglementaire, qui doivent être mis en œuvre par l'organisation. Les relations avec les autres autorités concernent les services collectifs, les services d'urgence, les fournisseurs d'électricité, la santé et la sécurité, comme la caserne de pompiers (pour la continuité d'activité), les opérateurs en télécommunication (pour le routage et la disponibilité) et les sociétés de distribution d'eau (pour le refroidissement du matériel).

5.6 Relations avec des groupes de travail spécialisés

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense

Mesure de sécurité

Il convient que l'organisation établisse et entretienne des relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles.

Objectif

Assurer la bonne circulation de l'information à l'égard de la sécurité.

Préconisations

Il convient d'envisager une inscription à des groupes de travail ou à des forums spécialisés aux fins suivantes :

a) mieux connaître les bonnes pratiques et se tenir informé de l'évolution des savoirs relatifs à la sécurité ;

b) s'assurer que la connaissance de l'environnement de la sécurité de l'information est à jour ;

c) recevoir rapidement des alertes, des conseils et des correctifs logiciels portant sur les attaques et les vulnérabilités ;

d) avoir accès à des conseils de spécialistes sur la sécurité de l'information ;

e) partager et échanger des informations sur les nouvelles technologies, les produits, les services, les menaces ou les vulnérabilités ;

f) mettre en place des relais d'information appropriés lors du traitement des incidents liés à la sécurité de l'information (voir 5.24 à 5.28).

Informations supplémentaires

Des accords de partage de l'information peuvent être établis en vue d'améliorer la coopération et la coordination dans le domaine de la sécurité. Il convient que de tels accords identifient les exigences en matière de protection des informations confidentielles.

5.7 Intelligence des menaces

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Identification #Détection	#Gestion_des_menaces_et_des_vulnérabilités	#Défense #Résilience

Mesure de sécurité

Il convient de recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces.

Objectif

Apporter une connaissance de l'environnement de menaces susceptible d'affecter l'organisation pour que celle-ci puisse prendre les mesures d'atténuation appropriées.

Préconisations

L'intelligence des menaces consiste à recueillir et analyser les informations relatives aux menaces existantes et émergentes de sorte à mettre en place les mesures de sécurité voulues pour empêcher les menaces de porter préjudice à l'organisation ou réduire leur impact.

L'intelligence des menaces peut être subdivisée en trois couches, qu'il convient de toutes prendre en compte :

a) intelligence des menaces stratégique : échange d'informations d'ordre général sur l'évolution des menaces (par exemple, types d'attaquants ou types d'attaques) ;

b) intelligence des menaces tactique : informations relatives aux méthodologies des attaquants, aux outils et aux technologies impliqués ;

c) intelligence des menaces opérationnelle : détails concernant des attaques spécifiques, y compris indicateurs techniques.

Il convient que l'intelligence des menaces soit :

a) pertinente (c'est-à-dire liée à la protection de l'organisation) ;

b) pointue (dans le sens où elle apporte à l'organisation une connaissance précise et détaillée des menaces) ;

c) contextuelle, pour donner conscience de la situation (en ajoutant du contexte aux informations par rapport à l'heure des événements, à l'emplacement où ils surviennent, aux expériences passées et à la prévalence dans des organisations similaires) ;

d) exploitable (c'est-à-dire que l'organisation peut agir rapidement et efficacement sur l'information).

Il convient d'inclure les activités suivantes dans l'intelligence des menaces :

a) établissement des objectifs en matière de production d'intelligence ;

b) identification, vérification et sélection des sources d'information internes et externes, nécessaires et appropriées pour fournir les informations requises en vue de la production d'intelligence ;

c) recueil d'informations auprès des sources sélectionnées, qui peuvent être internes et externes ;

d) traitement des informations recueillies pour les préparer à des fins d'analyse (par exemple, traduction, mise en forme ou corroboration des informations) ;

e) analyse des informations pour comprendre leur lien et leur importance vis-à-vis de l'organisation ;

f) communication et partage des informations aux personnes pertinentes sous une forme compréhensible.

Il convient que l'intelligence des menaces soit analysée puis utilisée :

a) en mettant en œuvre des processus pour intégrer les informations recueillies auprès des sources d'intelligence des menaces aux processus de gestion des risques liés à la sécurité de l'information de l'organisation ;

b) en tant que donnée d'entrée supplémentaire pour les mesures techniques, de prévention et de détection telles que les pare-feu, le système de détection des intrusions ou les solutions de protection contre les programmes malveillants ;

c) en tant que donnée d'entrée pour les processus et techniques de test de la sécurité de l'information.

Il convient que les organisations partagent mutuellement l'intelligence des menaces pour améliorer l'intelligence des menaces dans son ensemble.

Informations supplémentaires

Les organisations peuvent utiliser l'intelligence des menaces pour prévenir les menaces, les détecter ou y répondre. Les organisations peuvent produire une intelligence des menaces, mais le plus souvent, elles reçoivent et exploitent l'intelligence des menaces produite par d'autres sources.

L'intelligence des menaces est souvent proposée par des prestataires ou des conseillers indépendants, des agences gouvernementales ou des groupes d'intelligence des menaces collaboratifs.

L'efficacité de mesures de sécurité telles que 5.25, 8.7, 8.16 ou 8.22 dépend de la qualité des informations disponibles sur les menaces.

5.8 Sécurité de l'information dans la gestion de projet

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Gouvernance	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient d'intégrer la sécurité de l'information aux activités de gestion de projet de l'organisation.

Objectif

Assurer une prise en compte réelle et efficace des risques de sécurité de l'information liés aux projets et aux livrables dans les activités de gestion de projet, tout au long du cycle de vie des projets.

Préconisations

Il convient d'intégrer la sécurité de l'information aux activités de gestion de projet de l'organisation pour veiller à ce que les risques de sécurité de l'information soient pris en compte dans le cadre de la gestion de projet. Cette préconisation s'applique de manière générale à tout projet quel qu'il soit, indépendamment de la discipline ou du domaine d'application concerné, par exemple un projet lié à un processus clé de l'activité, aux technologies de l'information, à la gestion des installations et à d'autres processus sous-jacents. Il convient que les activités de gestion de projet en vigueur imposent que :

a) l'identification et la gestion des exigences en termes de sécurité de l'information (par exemple, exigences de sécurité des applications (8.26), exigences de conformité aux droits de propriété intellectuelle (5.32), etc.) ainsi que les processus associés concernant les livrables soient intégrés à un stade précoce des projets ;

b) les risques de sécurité de l'information soient appréciés et traités à un stade précoce puis de façon régulière dans le cadre des risques du projet, tout au long du cycle de vie du projet ;

c) les risques de sécurité de l'information associés à l'exécution des projets, tels que les aspects relatifs à la communication interne et externe, soient pris en compte et traités tout au long du cycle de vie du projet ;

d) des tests portant sur l'efficacité des mesures de sécurité de l'information soient réalisés ;

e) la sécurité de l'information soit intégrée à toutes les phases de la méthodologie de projet appliquée.

Il convient que la méthodologie de projet prenne en charge une façon structurée d'intégrer la sécurité de l'information, qu'il convient d'adapter en fonction de la gravité possible des risques de sécurité de l'information concernés, selon la nature du projet

Il convient de suivre l'adéquation des questions et activités liées à la sécurité de l'information par le biais de forums de gouvernance, tels que le comité de pilotage du projet, à des stades prédéfinis.

Pour tous les projets, il convient de traiter et de revoir régulièrement les incidences sur la sécurité de l'information. Il convient de déterminer et d'attribuer les responsabilités en matière de sécurité de l'information à des fonctions spécifiques définies dans les activités de gestion de projet.

Il convient de déterminer les exigences de sécurité de l'information à l'aide de plusieurs méthodes, telles que la prise en compte des exigences de conformité découlant de la politique de sécurité de l'information, des politiques portant sur des thèmes et des réglementations. D'autres exigences de sécurité de l'information peuvent être déterminées à partir d'activités telles que la modélisation des menaces, la revue des incidents, la définition de seuils de vulnérabilité ou la planification des mesures d'urgence, de sorte à garantir la protection de l'architecture et de la conception des systèmes d'information contre les menaces connues par rapport à l'environnement opérationnel.

Il convient que les exigences de sécurité de l'information et les mesures rendent compte de la valeur ajoutée de l'information concernée (voir 5.10, 5.12, 5.13), ainsi que des éventuels préjudices pour l'activité pouvant résulter de l'absence d'une sécurité adéquate.

Dans le cas d'un projet de développement agile, il convient d'intégrer les mesures et processus de sécurité de l'information requis à la version initiale du produit.

Il convient de déterminer les exigences de sécurité de l'information pour tous les types de projets, et de ne pas se limiter aux projets de développement de TIC. Il convient également d'examiner les lignes directrices suivantes lors de la détermination de ces exigences :

a) la nature de l'information concernée (détermination de l'information) et sa valeur correspondante en termes de sécurité (classification) ;

b) les besoins en matière de protection de l'information et les autres actifs concernés, notamment en termes de confidentialité, d'intégrité et de disponibilité ;

c) le niveau de confiance ou d'assurance requis en ce qui concerne l'identité déclarée des entités, afin d'en déduire les exigences d'authentification ;

d) les processus d'attribution de droits d'accès et d'autorisation pour les clients et les autres utilisateurs potentiels de l'organisation ainsi que pour les utilisateurs techniques ou dotés de privilèges, tels que les membres pertinents de l'équipe de projet, le personnel d'exploitation éventuel ou les fournisseurs externes ;

e) l'information des utilisateurs sur les tâches et les responsabilités qui leur incombent ;

f) les exigences découlant des processus de l'organisation, tels que la journalisation et la surveillance des transactions, les exigences de non-répudiation ;

g) les exigences prescrites par les autres mesures de sécurité, telles que les interfaces pour la journalisation et la surveillance ou les systèmes de détection de fuite de données ;

h) a conformité à l'environnement légal, statutaire, réglementaire et contractuel dans lequel l'organisation mène son activité ;

i) le niveau de confiance ou d'assurance requis pour les tiers afin de respecter la politique de sécurité de l'information et les politiques portant sur des thèmes de l'organisation, notamment les articles pertinents sur la sécurité des engagements ou accords éventuels.

Informations supplémentaires

Les projets sont par nature uniques, contrairement aux activités dictées par les processus, dans lesquelles les fonctions et les procédures ont, pour l'essentiel, été établies en vue d'une utilisation à long terme, favorisant la conformité aux mesures de sécurité de l'information. Avec une nouvelle organisation pour chaque projet, avec une tâche et un objectif uniques pouvant englober des activités expérimentales ou de développement, bien souvent avec une contrainte de délai, il convient que la méthodologie de projet prenne en charge une façon structurée d'intégrer la sécurité de l'information, qu'il convient d'adapter en fonction de la gravité possible des risques de sécurité de l'information concernés, selon la nature du projet.

Les méthodologies de gestion de projet relatives au développement de logiciel ou de systèmes qui sont prises en charge dans la présente mesure peuvent être des méthodologies de tous types, depuis le traditionnel développement en cascade jusqu'au développement agile, voire des méthodes moins structurées. La prise en compte précoce des exigences de sécurité de l'information concernant le produit ou le service, par exemple dès les phases de planification et de conception, peut permettre d'adopter des solutions plus efficaces et plus rentables du point de vue de la qualité et de la sécurité de l'information.

L'ISO/IEC 27005 fournit des recommandations sur l'utilisation des processus de gestion des risques en vue d'identifier les mesures permettant de satisfaire aux exigences de sécurité de l'information.

L'ISO 21500 fournit des recommandations sur les concepts et les processus de gestion de projet qui jouent un rôle déterminant pour les résultats des projets et ont une incidence sur ce dernier.

5.9 Inventaire des informations et des autres actifs associés

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gestion_des_actifs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient d'élaborer et de tenir à jour un inventaire des informations et des autres actifs associés, notamment les propriétaires.

Objectif

Identifier les informations de l'organisation et les autres actifs associés en vue de préserver la sécurité de l'information et d'en attribuer la propriété à qui de droit.

Préconisations

Inventaire

Il convient que l'organisation identifie ses informations et les autres actifs associés et qu'elle détermine leur importance en termes de sécurité de l'information. Il convient que la documentation soit tenue à jour dans des inventaires dédiés ou déjà en place selon le cas.

Il convient que l'inventaire des informations et des autres actifs associés soit exact, à jour, cohérent et en adéquation avec les autres inventaires. Les possibilités pour garantir l'exactitude d'un inventaire des informations et des autres actifs associés sont les suivantes :

a) mener des revues régulières des informations identifiées et des autres actifs associés par rapport à l'inventaire des actifs ;

b) appliquer automatiquement une mise à jour de l'inventaire au cours de l'installation, du changement ou du retrait d'un actif.

Il convient que l'emplacement de chaque actif soit indiqué dans l'inventaire au besoin.

Il n'est pas nécessaire que l'inventaire des actifs corresponde à une liste unique des informations et des autres actifs associés. Compte tenu du fait qu'il convient que l'inventaire des actifs soit géré par les fonctions pertinentes, on peut le considérer comme un ensemble d'inventaires dynamiques, tels qu'un registre des actifs informationnels, un inventaire du matériel, un inventaire des logiciels, un inventaire des MV, les installations, le personnel, les compétences, les capacités et les enregistrements.

Il convient de classifier chaque actif conformément à la classification de l'information (voir 5.12) qui lui est associée.

Il convient que la granularité de l'inventaire des informations et des autres actifs associés soit en adéquation avec les besoins de l'organisation. Dans certains cas, il n'est pas possible de documenter une instance d'actif spécifique dans le cycle de vie de l'information en raison de la nature de l'actif. Une instance de machine virtuelle dont le cycle de vie peut être limité dans la durée constitue un exemple d'actif à courte durée de vie. Néanmoins, il convient que les actifs associés figurent dans l'inventaire.

Propriété

Pour chaque information identifiée et autre actif associé, il convient d'attribuer la propriété de l'actif à une personne ou à un groupe ainsi que d'identifier la classification (voir 5.10, 5.12, 5.13). Il convient de mettre en œuvre un processus permettant de garantir l'attribution en temps et en heure d'un propriétaire à l'actif. Il convient d'attribuer un propriétaire aux actifs à leur création ou lorsqu'ils sont transférés à l'organisation. Il convient de réattribuer la propriété de l'actif, si nécessaire, lorsque son propriétaire actuel quitte l'organisation ou change de poste.

Tâches du propriétaire

Il convient que le propriétaire de l'actif soit responsable de la bonne gestion de cet actif tout au long de son cycle de vie, en veillant à ce que :

a) les informations et les autres actifs associés soient inventoriés ;

b) les informations et les autres actifs associés soient correctement classés et protégés ;

c) la classification fasse l'objet d'une revue régulière ;

d) les composants sous-jacents des actifs technologiques, tels que les composants et sous-composants logiciels, de base de données et de stockage, soient énumérés et liés ;

e) les exigences relatives à l'utilisation correcte des informations et des autres actifs associés (voir 5.10) soient définies ;

f) les restrictions d'accès correspondent à la classification, qu'elles soient effectives et qu'elles fassent l'objet d'une revue régulière ;

g) les actifs qui sont supprimés ou mis au rebut soient traités de manière sécurisée et retirés de l'inventaire ;

h) le propriétaire participe à l'identification et à la gestion des risques associés à son ou ses actifs ;

i) il soutienne les fonctions et les responsabilités dans la gestion de ses informations, par exemple les gestionnaires tels que le service informatique qui administre les informations métier.

Informations supplémentaires

L'inventaire des actifs permet de mettre en place une protection efficace et peut également s'avérer nécessaire à d'autres fins, par exemple dans le cadre de la santé et de la sécurité des personnes, des polices d'assurance ou pour des raisons financières. En outre, l'inventaire des actifs appuie la gestion des risques, les activités d'audit, la gestion des vulnérabilités et la planification du rétablissement.

Il est courant de réaliser des inventaires à plusieurs fins. Néanmoins, du point de vue de la sécurité de l'information, il convient qu'ils soient pertinents pour assurer la préservation de cette sécurité.

Le propriétaire identifié ne possède pas nécessairement de droits de propriété sur l'actif. Tel est, par exemple, le cas d'un service en nuage public que l'organisation utilise, mais dont les droits de propriété appartiennent au fournisseur de services en nuage, et sur lequel le propriétaire identifié n'a donc aucun droit de propriété.

Les tâches de routine peuvent être déléguées, par exemple à un dépositaire veillant quotidiennement aux actifs, mais la responsabilité des actifs demeure attachée au propriétaire.

Il peut s'avérer utile de désigner les groupes d'informations et les autres actifs associés qui agissent de pair pour assurer un service particulier. Dans ce cas, la délivrance du service, qui inclut les opérations d'actifs réalisées, est imputable au propriétaire du service.

Voir l'ISO/IEC 19770-1 pour de plus amples informations sur la gestion des actifs logiciels.

5.10 Utilisation correcte de l'information et des autres actifs associés

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient d'identifier, de documenter et de mettre en œuvre des règles d'utilisation correcte et des procédures de traitement de l'information et des autres actifs associés.

Objectif

Veiller à ce que l'information et les autres actifs associés soient correctement protégés, utilisés et traités.

Préconisations

Il convient que le personnel et les utilisateurs tiers qui utilisent ou ont accès à l'information et aux autres actifs associés de l'organisation soient informés des exigences de sécurité de l'information en vigueur pour la protection et le traitement de l'information et des autres actifs associés de l'organisation. Il convient qu'ils soient responsables de l'utilisation qu'ils font de toute ressource de traitement de l'information et de toute utilisation effectuée sous leur responsabilité.

Il convient que l'organisation établisse une politique portant sur le thème de l'utilisation correcte de l'information et des autres actifs associés et qu'elle communique les règles d'utilisation correcte à quiconque utilise ou traite l'information et les autres actifs associés. Il convient que la politique relative à l'utilisation correcte indique clairement la façon dont les personnes sont censées utiliser les actifs. Il est recommandé que la politique indique :

a) les comportements attendus de la part des personnes en matière de sécurité ;

b) les comportements inacceptables des personnes ;

c) l'utilisation autorisée de l'information et des autres actifs associés ;

d) l'utilisation interdite de l'information et des autres actifs associés ;

e) les activités de surveillance réalisées par l'organisation.

Il convient d'établir des procédures d'utilisation correcte pour le cycle de vie complet de l'information, en fonction de sa classification (voir 5.12) et des risques déterminés.

Il convient d'envisager les éléments suivants :

a) restreindre les accès pour renforcer les exigences de protection à chaque niveau de la classification ;

b) tenir à jour un enregistrement des personnes autorisées à recevoir les actifs ;

c) protéger les copies temporaires ou permanentes de l'information à un niveau en adéquation avec le niveau de protection de l'information originale ;

d) stocker les actifs associés à l'information conformément aux spécifications du fabricant (voir 7.8) ;

e) marquer clairement toutes les copies de support du nom de la personne autorisée à les recevoir (voir 7.10) ;

f) mettre en place une autorisation de mise au rebut d'actif et la ou les méthodes prises en charge.

Informations supplémentaires

Il peut arriver que les actifs concernés n'appartiennent pas directement à l'organisation, à l'instar des services en nuage publics. Il convient d'identifier l'utilisation de tels actifs externes et des actifs de l'organisation associés à ces actifs externes (par exemple, information, logiciel), le cas échéant, comme applicable et contrôlée, par exemple, par le biais d'accords dans le cas des fournisseurs de services en nuage.

5.11 Restitution des actifs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient que le personnel et les autres parties intéressées, au besoin, restituent tous les actifs de l'organisation qui sont en leur possession en cas de modification ou de rupture de leur relation de travail, contrat de travail ou engagement.

Objectif

Protéger les actifs de l'organisation dans le cadre du processus de modification ou de rupture d'une relation ou d'un contrat de travail.

Préconisations

Il convient de formaliser le processus de modification ou de rupture pour qu'il inclue la restitution de tous les actifs physiques et électroniques créés, appartenant à l'organisation ou lui ayant été confiés.

Si des membres du personnel et d'autres parties intéressées achètent du matériel à l'organisation ou utilisent leur propre matériel, il convient de suivre les procédures pour garantir que toutes les informations pertinentes sont tracées et transférées à l'organisation puis supprimées du matériel dans les règles (voir 7.14).

Dans les cas où des membres du personnel et d'autres parties intéressées détiennent des connaissances importantes pour les opérations en cours, il convient que cette information soit documentée et transmise à l'organisation.

Lors de la période de préavis, il convient que l'organisation empêche le personnel soumis au préavis d'effectuer des copies non autorisées d'informations pertinentes (en matière de propriété intellectuelle, par exemple) (voir 8.4).

Il convient que l'organisation identifie clairement et documente toutes les informations et les autres actifs associés à restituer, ce qui peut englober :

a) les terminaux utilisateurs ;

b) les dispositifs de stockage portables ;

c) les équipements spécialisés ;

d) le matériel d'authentification (par exemple, clés mécaniques, jetons physiques et cartes à puce) lié aux systèmes d'information, aux sites et aux archives physiques ;

e) les copies physiques d'informations.

Informations supplémentaires

Aucune autre information.

5.12 Classification de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Protection_des_informations	#Protection #Défense

Mesure de sécurité

Il convient de classifier l'information conformément aux besoins de l'organisation en termes de sécurité de l'information sur le plan de la confidentialité, de l'intégrité, de la disponibilité et des exigences des parties intéressées.

Objectif

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

Préconisations

Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème de la classification de l'information.

Il convient que l'organisation prenne en compte les exigences de confidentialité, d'intégrité et de disponibilité dans le plan de classification.

Il convient que la classification de l'information et les mesures de protection associées tiennent compte des besoins de l'organisation en matière de partage ou de limitation de l'information, pour protéger l'intégrité de l'information et en assurer la disponibilité, ainsi que des exigences légales concernant la confidentialité, l'intégrité ou la disponibilité de l'information. D'autres actifs que l'information peuvent également être classifiés conformément à la classification de l'information qu'ils stockent, traitent ou manipulent de quelque autre façon et qu'ils protègent.

Il convient que les propriétaires des informations soient responsables de leur classification.

Il convient que le plan de classification comporte des conventions de classification et des critères de revue de cette classification dans le temps. Il convient que les résultats de la classification soient mis à jour en fonction des évolutions de leur valeur, de leur sensibilité et du caractère critique des informations tout au long de leur cycle de vie.

Il convient d'établir un plan cohérent avec la politique portant sur le thème du contrôle d'accès (voir 5.15). Il convient que l'organisation s'assure que le plan de classification peut répondre aux besoins spécifiques de différents secteurs d'activité au sein de l'organisation.

La classification peut être déterminée en fonction de l'incidence qu'aurait sa compromission pour l'organisation. Il convient d'attribuer à chaque niveau défini dans le plan un nom significatif et logique dans le contexte de l'application du plan de classification.

Il convient que le plan soit identique pour toute l'organisation et qu'il figure dans ses procédures, de sorte que tout le monde puisse classifier l'information et les autres actifs associés de la même façon, comprenne les exigences de protection de la même manière et applique la protection appropriée.

Le plan de classification utilisé par l'organisation peut ne pas correspondre aux plans utilisés par d'autres organisations, même si les noms affectés aux niveaux sont similaires. En outre, la classification de l'information circulant entre les organisations peut varier en fonction du contexte de chaque organisation, même si les plans de classification sont identiques. Il convient donc que les accords conclus avec d'autres organisations incluant un partage d'information prévoient des procédures afin d'identifier la classification de cette information et d'interpréter les marques de classification apposées par ces autres organisations. La correspondance entre les différents plans peut être déterminée en recherchant une équivalence dans les méthodes de traitement et de protection associées.

Informations supplémentaires

La classification donne aux personnes qui travaillent avec l'information une indication concise sur la façon de la manipuler et de la protéger. Créer des groupes d'information ayant des besoins de protection similaires et spécifier les procédures de sécurité de l'information qui s'appliquent à toute l'information d'un groupe permet de résoudre les difficultés. Cette approche réduit la nécessité de procéder à une appréciation du risque au cas par cas et de concevoir des mesures individualisées.

L'information peut cesser d'être sensible ou critique après une période donnée, par exemple une fois qu'elle a été rendue publique. Il convient de prendre ces aspects en compte, car une surclassification peut entraîner la mise en œuvre de mesures inutiles et, in fine, des dépenses supplémentaires, ou à l'inverse, une sous-classification peut aboutir à des mesures de sécurité insuffisantes pour protéger l'information de toute compromission.

À titre d'exemple, un plan de classification de la confidentialité de l'information peut s'appuyer sur quatre niveaux, à savoir :

a) la divulgation ne cause aucun préjudice ;

b) la divulgation entraîne une atteinte mineure à la réputation ou un impact mineur sur le fonctionnement ;

c) la divulgation a, sur le court terme, des répercussions importantes sur les opérations ou les objectifs tactiques ;

d) la divulgation a, sur le long terme, des répercussions graves sur les objectifs stratégiques ou compromet la pérennité de l'organisation.

5.13 Marquage des informations

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Protection_des_informations	#Défense

Mesure de sécurité

Il convient d'élaborer et de mettre en œuvre un ensemble approprié de procédures pour le marquage de l'information, conformément au plan de classification de l'information adopté par l'organisation.

Objectif

Faciliter la communication de la classification de l'information et prendre en charge l'automatisation du traitement et du management de l'information.

Préconisations

Il convient que les procédures de marquage des informations et des autres actifs associés tiennent compte de tous les formats. Il convient que le marquage respecte le plan de classification défini en 5.12. Il convient que les marques soient facilement reconnaissables. Il convient que les procédures donnent des indications sur l'endroit et la façon dont les marques sont fixées, compte tenu de la manière dont on accède à l'information ou de la façon de manipuler les actifs, en fonction des types de support. Les procédures peuvent définir :

a) les cas pour lesquels le marquage n'est pas indispensable, par exemple dans le cas d'information non confidentielle en vue d'alléger la charge de travail ;

b) la façon de marquer les informations envoyées par ou stockées sur des moyens physiques ou électroniques, ou tout autre format ;

c) la façon de traiter les cas dans lesquels le marquage s'avère impossible, par exemple en raison de limitations techniques.

Il convient que l'information numérique utilise des métadonnées pour identifier, gérer et contrôler l'information, notamment du point de vue de la confidentialité. Il convient également que les métadonnées permettent d'effectuer une recherche efficace et correcte des informations. Il convient que les métadonnées favorisent les systèmes permettant d'interagir et de prendre des décisions selon le niveau de classification correspondant.

Il convient que les procédures décrivent la façon de rattacher les métadonnées aux informations, les marques à utiliser et la façon dont il convient de traiter les données en cohérence avec le modèle d'information et l'architecture informatique de l'organisation.

Il convient que les autres métadonnées pertinentes soient ajoutées par les systèmes lors du traitement de l'information, en fonction des propriétés de sécurité de l'information.

Il convient que le personnel et les autres parties intéressées soient sensibilisés aux procédures de marquage. Il convient que tout le personnel reçoive la formation requise de sorte que les informations soient correctement marquées et qu'elles soient traitées en conséquence.

Il convient que les données délivrées par des systèmes contenant de l'information classée comme sensible ou critique portent des marques appropriées.

Informations supplémentaires

Le marquage de l'information classée constitue une exigence clé dans les accords de partage d'information.

Les autres métadonnées qui peuvent être rattachées à l'information sont le processus organisationnel qui a créé l'information et la date/heure correspondante.

Le marquage de l'information et des autres actifs associés peut, parfois, avoir des conséquences négatives. Les actifs classifiés peuvent être plus faciles à identifier par des personnes malveillantes pour un mauvais usage éventuel.

Certains systèmes ne marquent pas les fichiers ou enregistrements de base de données individuels avec leur classification, mais protègent toutes les informations avec le niveau de classification le plus élevé de toutes les informations qu'ils contiennent ou peuvent contenir. Dans ces types de systèmes, il est habituel de déterminer puis de marquer l'information lorsqu'elle est exportée. S'il est interdit d'exporter l'information au-delà d'une classification donnée, la signature numérique et une technologie d'audit peuvent être utilisées pour que les personnes qui exportent une information moins classifiée soient tenues responsables de leurs actes.

Ci-dessous des exemples de techniques de marquage :

a) marquages matériels ;

b) en-têtes et pieds de page ;

c) métadonnées ;

d) filigrane ;

e) tampons en caoutchouc.

5.14 Transfert de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Protection

Mesure de sécurité

Il convient de mettre en place des règles, procédures ou accords de transfert de l'information, aussi bien au sein de l'organisation qu'entre l'organisation et des tierces parties, pour tous les types de fonctions de transfert.

Objectif

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

Préconisations

Généralités

Il convient que les règles, procédures et accords visant à protéger l'information pendant son transfert soient en adéquation avec la classification de l'information concernée. Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème du transfert de l'information. Dans les cas où l'information est transférée entre l'organisation et des tiers, il convient de définir et de gérer des accords (notamment authentification du destinataire) afin de protéger l'information sous toutes les formes en cours de transfert (voir 7.10).

Le transfert de l'information peut intervenir par le biais d'un transfert électronique, d'un transfert sur support physique et d'un transfert verbal.

Pour tous les types de transfert d'information, il convient d'intégrer aux règles, procédures et accords :

a) des mesures destinées à protéger l'information transférée contre l'interception, l'accès non autorisé, la reproduction, la modification, les erreurs d'acheminement, la destruction et le déni de service, y compris des niveaux de contrôle d'accès en accord avec la classification de l'information concernée et les éventuelles mesures particulières requises pour protéger l'information sensible, telles que l'utilisation de techniques de cryptographie (voir 8.24) ;

b) des mesures visant à garantir la traçabilité et la non-répudiation, notamment la gestion d'une chaîne de traçabilité pour l'information en cours de transfert ;

c) l'identification des contacts appropriés en lien avec l'accord de transfert, notamment les propriétaires de l'information, les propriétaires des risques, les responsables de la sécurité et les gestionnaires de l'information ;

d) les obligations et les responsabilités en cas d'incident de sécurité de l'information, comme la perte de supports physiques ou de données ;

e) l'utilisation convenue d'un système de marquage pour l'information sensible ou critique, permettant de garantir une compréhension immédiate des marques et la protection appropriée de l'information (voir 5.13) ;

f) la disponibilité et la fiabilité du service de transfert ;

g) la politique portant sur un thème ou les lignes directrices relatives à l'utilisation correcte des fonctions de transfert de l'information (voir 5.10) ;

h) les lignes directrices sur la conservation et la mise au rebut de tous les enregistrements commerciaux, dont les messages, conformément aux législations et réglementations nationales et locales applicables ;

i) la prise en compte de toutes les autres exigences légales, statutaires, réglementaires et contractuelles (voir 5.31, 5.32, 5.33, 5.34) en matière de transfert d'information, par exemple les exigences relatives aux signatures électroniques.

Transfert électronique

Il convient que les règles, procédures et accords prennent également en compte les éléments suivants dans le cadre de l'utilisation de moyens de communication électronique pour le transfert de l'information :

a) détection et protection contre les programmes malveillants qui peuvent être transmis via l'utilisation des communications électroniques (voir 8.7) ;

b) protection de l'information électronique sensible communiquée sous forme de pièce jointe ;

c) prévention de l'envoi de documents et de messages à une adresse ou un numéro erroné dans les communications ;

d) obtention d'une approbation avant d'utiliser des services externes publics comme une messagerie instantanée, un réseau social, le partage de fichiers ou le stockage en nuage ;

e) niveaux d'authentification plus élevés lors du transfert d'information par l'intermédiaire de réseaux accessibles au public ;

f) restrictions liées à l'utilisation des moyens de communication électronique, comme la prévention du renvoi automatique de courriers électroniques vers des adresses électroniques extérieures ;

g) recommandation au personnel et aux autres parties intéressées de ne pas envoyer de SMS ni de messages instantanés contenant des informations critiques dans la mesure où ces dernières peuvent être lues dans des lieux publics (et donc par des personnes non autorisées) ou stockées sur des dispositifs ne faisant pas l'objet de la protection adéquate ;

h) conseil au personnel et aux autres parties intéressées concernant l'utilisation des imprimantes ; d'intégrer la nécessité de récupérer les documents imprimés le plus vite possible, d'utiliser un code personnel à saisir sur l'imprimante si elle se trouve dans une autre pièce et de supprimer les numérisations et les impressions de la mémoire locale après une courte durée ;

i) information du personnel et des autres parties intéressées sur les problèmes liés à l'utilisation de télécopieurs ou de services de télécopie, à savoir :

   1) l'accès non autorisé aux mémoires de messages intégrées pour récupérer des messages ;

   2) la programmation délibérée ou accidentelle de machines pour qu'elles envoient des messages à des numéros précis.

Transfert physique des supports

Lors du transfert de supports physiques, y compris papier, il convient également que les règles, procédures et accords tiennent compte des points suivants :

a) les responsabilités en matière de contrôle et d'information de la transmission, de l'expédition et de la réception ;

b) la qualité de l'adressage et du transport du message ;

c) les normes techniques minimales pour l'encapsulation et la transmission, par exemple l'utilisation d'enveloppes opaques ;

d) les normes d'identification coursiers ;

e) la liste approuvée des tiers prestataires de services de transport ou de coursiers selon la classification de l'information.

Transfert verbal

Pour protéger le transfert verbal de l'information, il convient de rappeler au personnel et aux autres parties intéressées qu'il est recommandé de :

a) ne pas tenir de conversations confidentielles dans des lieux publics ou via des canaux de communication non sécurisés dans la mesure où ces dernières peuvent être écoutées par des personnes non autorisées ;

b) ne pas laisser de messages comportant une information confidentielle sur des répondeurs ni de messages vocaux dans la mesure où ces derniers peuvent être réécoutés par des personnes non autorisées, stockés sur des systèmes à usage collectif ou incorrectement mémorisés à la suite d'une erreur de numérotation ;

c) faire l'objet d'un examen jusqu'au niveau approprié pour écouter la conversation ;

d) mettre en œuvre les mesures appropriées par salle, par exemple insonorisation, fermeture de porte ;

e) débuter toute conversation sensible par une exonération de responsabilité afin que les personnes présentes connaissent le niveau de classification et les éventuelles exigences de manipulation de l'information qu'ils sont sur le point d'entendre.

Informations supplémentaires

Le transfert de l'information peut intervenir par le biais de différents types de moyens de transfert, dont des interfaces automatiques, le courrier électronique, l'échange de données électroniques, les réseaux sociaux, les services de messagerie instantanée, la voix et la télécopie.

5.15 Contrôle d'accès

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient de définir et de mettre en œuvre des règles visant à gérer l'accès physique et logique à l'information et aux autres actifs associés en fonction des exigences métier et de sécurité de l'information.

Objectif

Garantir l'accès par le biais d'autorisations et empêcher l'accès non autorisé à l'information et aux autres actifs associés.

Préconisations

Il convient que les propriétaires des informations et des autres actifs associés déterminent les exigences métier et de sécurité de l'information relatives au contrôle d'accès et qu'ils définissent une politique portant sur le thème du contrôle d'accès, puis qu'ils communiquent ces éléments à toutes les parties prenantes pertinentes, telles que les utilisateurs et les propriétaires de services.

Il convient que ces exigences et cette politique comprennent les points suivants :

a) détermination des entités qui nécessitent un type d'accès défini aux actifs ;

b) sécurité des applications (8.26) ;

c) accès physique qui doit être pris en charge par des mesures d'accès physique adéquates (voir 7.2, 7.3, 7.4) ;

d) diffusion de l'information et autorisations, par exemple principe du besoin d'en connaître, niveaux de sécurité de l'information et classification de l'information (voir 5.10, 5.12, 5.13) ;

e) restrictions liées aux privilèges d'accès (voir 8.2) ;

f) séparation des tâches (voir 5.3) ;

g) législation et obligations contractuelles applicables en matière de limitation de l'accès aux données ou aux services (voir 5.31, 5.32, 8.3, 5.33, 5.34) ;

h) cloisonnement des fonctions de contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès ;

i) autorisation formelle des demandes d'accès (voir 5.16 et 5.18) ;

j) gestion des droits d'accès (voir 5.18) ;

k) journalisation (voir 8.15).

Il convient de mettre en œuvre des règles de contrôle d'accès en définissant et en affectant les droits d'accès et les restrictions appropriées aux entités pertinentes. Une entité peut correspondre à un utilisateur humain aussi bien qu'à un élément technique ou logique, par exemple une machine, un équipement ou un service. Pour simplifier la gestion du contrôle d'accès, des fonctions spécifiques peuvent être affectées à des groupes d'entités.

Il convient de prendre en compte les points suivants lors de la mise en œuvre de règles de contrôle d'accès :

a) cohérence entre les droits d'accès et la classification de l'information ;

b) cohérence entre les droits d'accès et les besoins et exigences de sécurité du périmètre physique ;

c) en tenant compte de tous les types de connexions disponibles dans les environnements répartis pour définir leurs règles de contrôle d'accès, il convient que les entités se voient uniquement accorder l'accès à l'information et aux autres actifs associés, dont les réseaux et services en réseau, qu'elles ont l'autorisation d'utiliser.

Informations supplémentaires

On a souvent recours à des principes globaux dans le contexte du contrôle d'accès. Les deux principes les plus couramment utilisés sont les suivants :

a) le besoin d'en connaître : une entité a uniquement accès à l'information dont elle a besoin pour réaliser les tâches qui lui incombent (différentes tâches ou fonctions impliquent des besoins d'en connaître différents, d'où des profils d'accès différents) ;

b) le besoin d'utiliser : une entité a uniquement accès à l'infrastructure informatique qui lui est à l'évidence nécessaire.

Il convient de faire preuve de prudence lors de la spécification des règles de contrôle d'accès :

a) établir des règles fondées sur le principe du moindre privilège : « Tout est généralement interdit sauf autorisation expresse » plutôt que sur la règle, moins fiable, selon laquelle « Tout est généralement autorisé sauf interdiction expresse » ;

b) tenir compte des modifications apportées automatiquement aux étiquettes (voir 5.13) par les moyens de traitement de l'information et des modifications qui sont à l'appréciation de l'utilisateur ;

c) examiner les modifications apportées automatiquement aux droits d'accès de l'utilisateur par le système d'information et les modifications qui sont décidées par un administrateur ;

d) déterminer quand il convient que l'approbation soit définie et revue régulièrement.

Il convient que les règles de contrôle d'accès s'appuient sur des procédures documentées (voir 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) et des responsabilités définies (voir 5.2, 5.17).

Il existe plusieurs façons de mettre en œuvre le contrôle d'accès, telles que MAC (Mandatory Access Control ou contrôle d'accès obligatoire), DAC (Discretionary Access Control ou contrôle d'accès discrétionnaire) et RBAC (Role-Based Access Control ou contrôle d'accès basé sur les rôles).

Les règles de contrôle d'accès peuvent également contenir des éléments dynamiques, par exemple une fonction qui évalue les accès antérieurs ou des valeurs de l'environnement spécifiques. Les règles de contrôle d'accès peuvent être mises en œuvre en différentes granularités, allant de la couverture de réseaux ou systèmes complets jusqu'à des champs de données spécifiques. Elles peuvent également prendre en compte des propriétés telles que le site de l'utilisateur ou le type de connexion réseau utilisé pour l'accès. Ces principes et le mode de définition du contrôle d'accès granulaire peuvent avoir d'importantes répercussions sur les coûts. De façon générale, plus les règles sont strictes et la granularité importante, plus le coût est élevé.

Il convient de s'appuyer sur les exigences métier et les risques à prendre en compte pour définir les règles de contrôle d'accès à appliquer et la granularité requise.

5.16 Gestion des identités

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient de gérer le cycle de vie complet des identités.

Objectif

Permettre l'identification univoque des personnes et des systèmes qui accèdent à l'information de l'organisation et aux autres actifs associés, ainsi que l'affectation des droits d'accès appropriés.

Préconisations

Il convient que les processus utilisés dans le contexte de la gestion des identités offrent les garanties suivantes :

a) pour les identités affectées aux personnes, une identité donnée n'est liée qu'à une seule personne, ce qui permet de la tenir responsable des actes effectués sous son identité ;

b) les identités affectées à plusieurs personnes (comme les identités partagées) sont uniquement autorisées dans les cas où elles s'avèrent nécessaires pour des raisons opérationnelles ou liées à l'activité ; elles sont soumises à une approbation et une documentation spécifiques ;

c) les identités affectées à des entités non humaines sont soumises à une approbation et une supervision indépendante continue séparées en conséquence ;

d) les identités sont rapidement désactivées ou supprimées si elles ne sont plus nécessaires, par exemple si les entités associées sont supprimées ou ne sont plus utilisées, ou si la personne liée à une identité a quitté l'organisation ou changé de fonction et qu'elle ne possède plus l'identité ;

e) dans un domaine spécifique, une identité donnée est affectée à une seule et unique entité, c'est-à-dire qu'il n'est pas possible d'affecter plusieurs identités à une même entité au sein d'un contexte donné (identités en double) ;

f) les enregistrements de tous les événements significatifs concernant l'utilisation et la gestion des identités des utilisateurs ainsi que les informations d'authentification sont archivés.

Il convient que les organisations mettent en place un processus sous-jacent pour gérer les modifications apportées aux identités des personnes, notamment pour opérer des vérifications par rapport aux documents de confiance et disposer d'un moyen de mettre à jour leur identité « professionnelle » (carte d'accès et compte réseau) conformément à la nouvelle identité, au lieu d'annuler leur identité actuelle et d'en créer une nouvelle.

Il convient que l'organisation veille à mettre en place l'appréciation du risque et les mesures de sécurité nécessaires lors de l'utilisation d'identités et de justificatifs d'identité fournis par des tiers (par exemple, justificatifs d'identité de médias sociaux).

Informations supplémentaires

Accorder ou supprimer l'accès à l'information ou aux actifs associés constitue en général une procédure à plusieurs étapes :

a) confirmer les exigences métier en vue de l'établissement d'une identité ;

b) vérifier l'identité d'une entité avant de lui attribuer une identité logique ;

c) établir une identité ;

d) configurer et activer l'identité. Cela implique également la configuration et le paramétrage initial des services d'authentification liés ;

e) accorder des droits d'accès spécifiques à l'identité ou annuler ces mêmes droits, en s'appuyant sur les décisions d'autorisation ou d'habilitation appropriées (voir 5.18).

5.17 Informations d'authentification

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient que l'attribution et la gestion des informations d'authentification soient contrôlées par un processus de gestion, impliquant l'information du personnel quant au traitement approprié des informations d'authentification.

Objectif

Assurer l'authentification de l'entité concernée et éviter toute défaillance des processus d'authentification.

Préconisations

Attribution d'informations d'authentification

Il convient que le processus d'attribution et de gestion garantisse :

a) que les mots de passe personnels ou les codes PIN générés automatiquement au cours des processus d'inscription ainsi que les informations d'authentification temporaires soient impossibles à deviner et uniques pour chaque personne ; et qu'ils soient modifiés par l'utilisateur après la première utilisation ;

b) que des procédures soient mises en place pour vérifier l'identité d'un utilisateur avant d'attribuer de nouvelles informations d'authentification ou des informations d'authentification de remplacement ou temporaires ;

c) que les informations d'authentification, y compris temporaires, soient transmises aux utilisateurs de manière sécurisée (par exemple, via un canal authentifié et protégé) ; que l'utilisation de courriers électroniques (en texte clair) non protégés soit évitée ;

d) que les utilisateurs accusent réception des informations d'authentification ;

e) que les informations d'authentification par défaut définies par les constructeurs et éditeurs soient modifiées après installation des systèmes ou logiciels ;

f) que les enregistrements des informations d'authentification et de tous les événements significatifs concernant leur attribution et leur gestion soient conservés et qu'un caractère confidentiel leur soit accordé ; et que la méthode de conservation des enregistrements soit approuvée (par exemple par le biais d'un outil de type coffre-fort pour mots de passe approuvés).

Responsabilités des utilisateurs

Il convient de donner les conseils suivants à toute personne amenée à consulter ou à utiliser des informations d'authentification :

a) tous les utilisateurs qui ont accès à des informations d'authentification secrètes sont informés du fait qu'ils doivent garder ces informations confidentielles. Les informations d'authentification secrètes personnelles, comme les mots de passe, ne doivent être communiquées à personne. Les informations d'authentification secrètes utilisées dans le contexte des identités liées à plusieurs utilisateurs ou liées à des entités non personnelles sont uniquement communiquées aux personnes autorisées. L'obligation de suivre ces règles est également indiquée dans les conditions générales d'embauche (voir 6.2) ;

b) les informations d'authentification affectées ou compromises sont immédiatement modifiées s'il existe un signe de compromission ;

c) en cas d'utilisation de mots de passe comme informations d'authentification, choisir des mots de passe de bonne qualité et, du côté de l'organisation, suivre les toutes dernières recommandations des bonnes pratiques pour éviter toute violation des mots de passe, par exemple :

   1) ne pas les composer par rapport à une information personnelle facile à deviner ou à obtenir, par exemple : noms, numéros de téléphone et dates d'anniversaire ;

   2) ne pas utiliser de mots du dictionnaire ni de combinaisons de ces derniers ;

   3) utiliser des phrases secrètes faciles à retenir et essayer d'y inclure des caractères alphanumériques et spéciaux ;

   4) appliquer une longueur minimale ;

d) ne pas utiliser les mêmes informations d'authentification dans les différents mécanismes d'authentification ;

e) utiliser des informations d'authentification différentes selon les identités pour garantir l'imputabilité.

Système de gestion des mots de passe

Lorsque des mots de passe sont utilisés comme informations d'authentification, il convient que le système de gestion des mots de passe :

a) autorise l'utilisateur à choisir et à modifier ses mots de passe, et prévoie une procédure de confirmation pour prendre en compte les erreurs de saisie ;

b) impose le choix de mots de passe forts (voir c) sous la « responsabilité des utilisateurs ») ;

c) impose aux utilisateurs de changer leur mot de passe à la première connexion ;

d) impose des changements de mots de passe si besoin, par exemple après un incident de sécurité, ou lors de la fin ou de la modification du contrat de travail, lorsqu'un utilisateur a des mots de passe connus pour des identités demeurant actives (par exemple, des identités partagées) ;

e) tienne à jour un enregistrement des anciens mots de passe et empêche leur réutilisation ;

f) empêche l'utilisation des mots de passe couramment utilisés et des noms d'utilisateurs publiés, ainsi que des combinaisons de mots de passe en provenance de systèmes piratés ;

g) n'affiche pas les mots de passe à l'écran lors de leur saisie ;

h) stocke les fichiers de mots de passe à d'autres emplacements que les données d'application système ;

i) stocke et transmette les mots de passe sous une forme protégée.

Il convient d'opérer un chiffrement et un hachage des mots de passe conformément aux techniques de cryptographie approuvées pour les mots de passe (voir 8.24).

Informations supplémentaires

Les mots de passe ou les phrases secrètes sont un type courant d'informations d'authentification et constituent un moyen usuel de vérifier l'identité d'un utilisateur. Les codes PIN, les clés cryptographiques et autres données stockées sur des jetons matériels (par exemple, des cartes à puce) qui produisent des codes d'authentification constituent d'autres types d'informations d'authentification. De plus amples informations sont disponibles dans l'ISO/IEC 24760 (toutes les parties).

Imposer une fréquente modification des mots de passe peut s'avérer problématique et risquer d'ennuyer les utilisateurs, qui peuvent alors oublier les nouveaux mots de passe, les noter à des endroits peu sûrs ou choisir des mots de passe non sécurisés. La mise à disposition du Single Sign On (SSO, l'authentification unique) ou d'autres outils de gestion de l'authentification limite la quantité d'informations d'authentification que les utilisateurs doivent protéger et peut ainsi améliorer l'efficacité de cette mesure. Cependant, ces outils peuvent également aggraver les conséquences découlant de la divulgation des informations d'authentification.

Certaines applications nécessitent que l'attribution de mots de passe aux utilisateurs soit réalisée par une autorité indépendante ; dans ce cas, les points a), c) et d) au-dessous de « Système de gestion des mots de passe » des préconisations qui précèdent ne s'appliquent pas.

5.18 Droits d'accès

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient que les droits d'accès à l'information et aux autres actifs associés soient mis en service, révisés, modifiés et supprimés conformément à la politique portant sur le thème de l'organisation et aux règles de contrôle d'accès.

Objectif

Garantir l'accès à l'information et aux autres actifs associés par le biais d'autorisations seulement.

Préconisations

Attribution et révocation des droits d'accès

Il convient que le processus d'attribution ou de révocation des droits d'accès physiques et logiques accordés à une identité authentifiée dans une entité inclue :

a) l'obtention de l'autorisation d'utilisation du système d'information ou du service de la part du propriétaire de ce système d'information ou de ce service (voir 5.9) ; une approbation distincte des droits d'accès par la direction peut également s'avérer appropriée ;

b) la prise en compte de la séparation des tâches, notamment la séparation des fonctions d'approbation et de mise en œuvre des droits d'accès, et la séparation des fonctions incompatibles ;

c) l'assurance que les droits d'accès sont supprimés lorsqu'une personne n'a plus besoin d'accéder aux systèmes d'information ou aux services, en particulier l'assurance d'une suppression rapide des droits d'accès des utilisateurs qui ont quitté l'organisation ;

d) la vérification que le niveau d'accès accordé est adapté aux politiques d'accès portant sur des thèmes (voir 5.15) et qu'il est cohérent avec les autres exigences de sécurité de l'information telles que la séparation des tâches (voir 5.3) ;

e) l'assurance que les droits d'accès ne sont activés (par exemple, par les fournisseurs de services) qu'une fois les procédures d'autorisation achevées ;

f) la tenue à jour d'un enregistrement centralisé de tous les droits d'accès accordés aux identifiants utilisateurs (logiques ou physiques) pour leur permettre d'accéder à l'information, aux systèmes d'information et aux services ;

g) la modification des droits d'accès des utilisateurs qui ont changé de fonction ou de poste ;

h) la suppression ou l'adaptation des droits d'accès physiques et logiques. Cela peut être réalisé par suppression, révocation ou remplacement des clés, des informations d'authentification, des cartes d'identification ou des abonnements.

Revue des droits d'accès

Il convient que les revues régulières des droits d'accès physiques et logiques tiennent compte de ce qui suit :

a) les droits d'accès des utilisateurs consécutivement à un changement quelconque au sein de la même organisation (par exemple, promotion ou rétrogradation) ou à la fin du contrat de travail (voir 6.1 à 6.5) ;

b) autorisations relatives aux privilèges d'accès ;

c) journalisation des changements apportés aux droits d'accès physiques et logiques des utilisateurs.

Points à prendre en compte avant la modification ou la fin du contrat de travail

Il convient que les droits d'accès à l'information et aux autres actifs associés d'un utilisateur soient révisés et adaptés ou supprimés avant toute modification ou fin du contrat de travail en fonction de l'évaluation des facteurs de risque suivants :

a) s'agit-il d'une rupture ou d'une modification du contrat intervenue à l'initiative de l'utilisateur, de l'utilisateur tiers ou de la direction, et quel en est le motif ?

b) quelles sont les responsabilités de l'utilisateur, de l'utilisateur tiers ou tout autre utilisateur ?

c) quelle est la valeur des actifs accessibles ?

Informations supplémentaires

Il convient d'envisager d'établir des rôles d'accès utilisateur en fonction des exigences métier, qui regroupent des droits d'accès dans des profils d'utilisateurs types. Les requêtes et les revues d'accès (voir 5.17) sont plus faciles à gérer au niveau de ce type de rôles qu'au niveau des droits d'accès individuels.

Il convient d'envisager d'inclure des clauses dans les contrats de travail et les contrats de service, stipulant les sanctions encourues en cas de tentative d'accès non autorisé par le personnel (voir 6.2, 6.4, 6.6, 5.20).

Des droits d'accès temporaires peuvent permettre de gérer efficacement et de manière proactive l'accès à l'information et aux ressources, par exemple en fonction du rôle de l'utilisateur. Dans ce cas, il convient que les droits d'accès soient accordés pour une période limitée puis révoqués à la date d'expiration.

Lorsque la direction est à l'origine de la rupture du contrat de travail, le personnel ou les utilisateurs tiers mécontents peuvent chercher délibérément à altérer l'information ou à saboter les moyens de traitement de l'information. S'il s'agit de personnes qui démissionnent ou qui sont licenciées, elles peuvent être tentées de recueillir des informations en vue d'une utilisation ultérieure.

Le clonage constitue un moyen efficace pour les organisations d'attribuer des droits d'accès aux utilisateurs. Néanmoins, il convient de l'effectuer avec soin par rapport aux différents rôles identifiés par l'organisation plutôt que de se contenter de cloner une identité avec tous les droits d'accès associés. Le clonage comporte le risque inhérent d'engendrer des droits d'accès excessifs à l'information et aux actifs associés.

5.19 Sécurité de l'information dans les relations avec les fournisseurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient d'identifier et de mettre en œuvre des processus et procédures pour gérer les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services du fournisseur.

Objectif

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

Préconisations

Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème des relations avec les fournisseurs.

Il convient que l'organisation identifie et mette en œuvre des processus et procédures visant à traiter les risques de sécurité associés à l'utilisation des produits et services mis à disposition par les fournisseurs. Il convient d'appliquer également ce principe à l'utilisation par l'organisation des ressources des fournisseurs de services en nuage. Il convient que ces processus et procédures comprennent ceux que l'organisation doit mettre en œuvre, ainsi que ceux que l'organisation demande au fournisseur de mettre en œuvre pour commencer à utiliser les produits ou les services du fournisseur, ou pour cesser d'utiliser les produits ou les services du fournisseur, dont :

a) l'identification et la documentation des types de fournisseurs, par exemple services de TIC, services logistiques, services collectifs, services financiers, composants de l'infrastructure TIC, qui peuvent compromettre la confidentialité, l'intégrité et la disponibilité de l'information dans l'organisation ;

b) l'évaluation et la sélection des produits ou des services du fournisseur qui présentent les mesures de sécurité adéquates et leur revue ; en particulier, la précision et l'exhaustivité des mesures mises en œuvre par le fournisseur pour assurer l'intégrité de son information et du traitement afférent, et par conséquent la sécurité de l'information de l'organisation ;

c) la définition de l'information, des services de TIC et de l'infrastructure physique de l'organisation à laquelle les fournisseurs peuvent accéder et qu'ils peuvent surveiller, contrôler ou utiliser ;

d) la définition des types de composants et de services de l'infrastructure TIC mis à disposition par les fournisseurs, qui peuvent compromettre la confidentialité, l'intégrité et la disponibilité de l'information dans l'organisation ;

e) l'appréciation et la gestion des risques de sécurité de l'information associés aux aspects suivants :

    1) utilisation par les fournisseurs de l'information de l'organisation et des autres actifs associés, y compris les risques occasionnés par le personnel potentiellement malveillant du fournisseur ;

    2) dysfonctionnement ou vulnérabilités des produits (y compris les composants et sous-composants logiciels utilisés dans lesdits produits) ou des services mis à disposition par les fournisseurs ;

f) la surveillance de la conformité aux exigences de sécurité de l'information établies pour chaque type de fournisseur et chaque type d'accès, incluant une revue et une validation des produits par une tierce partie ;

g) l'atténuation de la non-conformité d'un fournisseur, qu'elle ait été détectée par le biais de la surveillance ou d'un autre moyen ;

h) le traitement des incidents et des impondérables associés aux produits et services des fournisseurs, dont les responsabilités de l'organisation et celles des fournisseurs ;

i) les dispositions de résistance et, si nécessaire, de récupération et de secours pour garantir la disponibilité de l'information du fournisseur et du traitement de l'information opéré par le fournisseur, et par conséquent la disponibilité de l'information de l'organisation ;

j) la sensibilisation et la formation du personnel de l'organisation en interaction avec le personnel du fournisseur, sur les règles appropriées d'engagement, les politiques portant sur des thèmes, les processus et procédures, et le comportement en fonction du type de fournisseur et du niveau d'accès du fournisseur aux systèmes et à l'information de l'organisation ;

k) la gestion des transitions nécessaires de l'information, des actifs associés et de tout ce qui doit être modifié en général, et l'assurance que la sécurité de l'information est préservée tout au long de la période de transition ;

l) les exigences visant à préserver la sécurité lors de la rupture de la relation avec le fournisseur, dont :

    1) la suppression des droits d'accès attribués ;

    2) le traitement de l'information ;

    3) la détermination du détenteur de la propriété intellectuelle créée au cours de l'engagement ;

    4) la portabilité de l'information en cas de changement de fournisseur ou d'internalisation ;

    5) le contrôle d'accès ;

    6) la gestion des enregistrements ;

    7) la restitution des actifs ;

    8) l'élimination sécurisée de l'information, et ;

    9) les exigences permanentes de confidentialité ;

m) les attentes en matière de sécurité du personnel et de sécurité physique du personnel et des installations du fournisseur.

Il convient de prendre en compte les procédures de continuité du traitement dans le cas où le fournisseur ne serait plus en mesure de fournir ses produits ou ses services (par exemple, en raison d'un incident, de la cessation d'activité du fournisseur ou de l'arrêt de la production de certains composants suite à des avancées technologiques) afin d'éviter tout retard dans la mise en place des produits ou des services de remplacement (par exemple, identification anticipée d'un autre fournisseur ou recours permanent à d'autres fournisseurs).

Informations supplémentaires

Dans les cas où une organisation n'aurait pas la possibilité d'imposer des exigences à un fournisseur, il convient que l'organisation :

a) tienne compte des préconisations données ci-dessus pour prendre les décisions relatives au choix d'un fournisseur et de son service ;

b) mette en œuvre des mesures compensatoires, si besoin, en s'appuyant sur une appréciation du risque.

En gérant la sécurité de l'information de manière inadaptée, les fournisseurs peuvent rendre l'information vulnérable. Il convient d'identifier et d'appliquer des mesures pour gérer l'accès des fournisseurs à l'information et aux moyens de traitement de l'information. Par exemple, s'il existe un besoin particulier de confidentialité de l'information, il est possible de mettre en place des engagements de non-divulgation. Un autre exemple concerne les risques liés à la protection des données à caractère personnel lorsque l'accord conclu avec le fournisseur implique un transfert de l'information ou un accès à l'information au-delà des frontières. Il est nécessaire que l'organisation soit pleinement consciente que la responsabilité légale ou contractuelle de protection de l'information lui incombe.

Les risques peuvent également découler de l'inadéquation des mesures liées aux composants de l'infrastructure TIC ou aux services assurés par les fournisseurs. Le dysfonctionnement ou la vulnérabilité de composants ou de services peuvent entraîner des violations de sécurité de l'information dans l'organisation ou dans une autre entité, par exemple via une infection par un logiciel malveillant, des attaques ou d'autres dommages sur des entités autres que l'organisation.

Voir l'ISO/IEC 27036-2 pour de plus amples informations.

5.20 Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient de mettre en place les exigences de sécurité de l'information pertinentes et d'en convenir avec chaque fournisseur, en fonction du type de relation avec le fournisseur.

Objectif

Garantir la sécurité de l'information de l'organisation dans le cadre des relations avec les fournisseurs.

Préconisations

Il convient de rédiger et de documenter les accords avec les fournisseurs de sorte à s'assurer de la bonne compréhension de l'organisation et du fournisseur de leur obligation mutuelle à satisfaire aux exigences de sécurité de l'information applicables.

Pour satisfaire aux exigences de sécurité de l'information identifiées, il convient d'envisager d'inclure les conditions suivantes dans l'accord :

a) description de l'information à fournir ou à laquelle l'accès doit être rendu possible et des méthodes utilisées pour fournir cette information ou y accéder ;

b) classification de l'information conformément au plan de classification de l'organisation (voir 5.10, 5.12, 5.13) ;

c) mise en correspondance du plan de classification propre à l'organisation et du plan de classification du fournisseur ;

d) exigences légales, statutaires, réglementaires et contractuelles, y compris la protection des données, le traitement des données à caractère personnel (DCP), les droits de propriété intellectuelle et les droits d'auteur, et la description de la méthode appliquée pour en assurer le respect ;

e) obligation pour chaque partie au contrat de mettre en œuvre un ensemble convenu de mesures, dont le contrôle d'accès, la revue des performances, la surveillance, la génération de rapports et l'audit ; ainsi que l'obligation pour le fournisseur de se conformer aux exigences de sécurité de l'organisation ;

f) règles d'utilisation correcte de l'information, y compris, si nécessaire, les conditions d'utilisation incorrecte ;

g) procédures ou conditions relatives à l'octroi ou au retrait des autorisations liées à l'utilisation de l'information de l'organisation par le personnel du fournisseur, par exemple par le biais d'une liste explicite du personnel du fournisseur autorisé à utiliser l'information de l'organisation ;

h) exigences de sécurité de l'information pertinentes pour le contrat concerné, dont les exigences de sécurité de l'information relatives à l'infrastructure TIC du fournisseur ; en particulier, exigences minimales en termes de sécurité de l'information pour chaque type d'information et type d'accès devant constituer la base des accords avec les fournisseurs, par rapport aux besoins de l'organisation et à ses critères de risque ;

i) conditions dans lesquelles les exigences et les mesures de sécurité de l'information seront documentées dans un accord signé par les deux parties ;

j) indemnités et actions correctives en cas de manquement du contractant à satisfaire aux exigences ;

k) exigences et procédures de gestion des incidents (notamment la notification et la collaboration lors de l'action corrective) ;

l) exigences de formation et de sensibilisation aux procédures et aux exigences de sécurité de l'information spécifiques, par exemple réponse aux incidents et procédures d'autorisation ;

m) réglementations applicables à la sous-traitance, notamment les mesures qu'il est nécessaire de mettre en œuvre, comme un accord relatif au recours à des sous-traitants, qui exige que ceux-ci soient soumis aux mêmes obligations que le fournisseur, exige la communication d'une liste des sous-traitants et une notification préalablement à tout changement ;

n) partenaires concernés, avec un contact pour les questions liées à la sécurité de l'information ;

o) les exigences de présélection, le cas échéant, du personnel du fournisseur, notamment les responsabilités liées aux procédures de présélection et de notification si la présélection n'a pas abouti ou si les résultats sont source d'inquiétude ou de doute ;

p) les mécanismes de preuve et d'assurance des attestations de tierce partie concernant les exigences de sécurité de l'information liées aux processus des fournisseurs et un rapport indépendant sur l'efficacité des mesures de sécurité ;

q) le droit de contrôler les processus et les mesures de sécurité du fournisseur en rapport avec le contrat ;

r) l'obligation pour le fournisseur de communiquer périodiquement un rapport sur l'efficacité des mesures et son accord pour appliquer rapidement les actions correctives aux problèmes signalés dans le rapport ;

s) les processus de correction des défauts et de résolution des conflits ;

t) la mise à disposition d'un processus de sauvegarde en adéquation avec les besoins de l'organisation (en termes de fréquence, de type et d'emplacement de stockage) ;

u) la garantie de disponibilité d'une installation alternative (un site de récupération après sinistre) qui ne soit pas soumise aux mêmes menaces que l'installation principale ni à des considérations de repli (mesures de sécurité alternatives) en cas d'échec des mesures principales ;

v) un processus de gestion des changements qui assure la notification préalable de l'organisation et permette à cette dernière de ne pas accepter les changements ;

w) des mesures de sécurité physique en accord avec la classification de l'information ;

x) des mesures de transfert de l'information destinées à protéger l'information au cours du transfert physique ou de la transmission logique ;

y) des clauses de résiliation lors de la conclusion du contrat, incluant la gestion des enregistrements, la restitution des actifs, l'élimination sécurisée de l'information et la confidentialité permanente ;

z) mise à disposition d'une méthode de destruction sécurisée des informations de l'organisation stockées par le fournisseur dès qu'elles ne sont plus utiles ;

aa) à la fin du contrat, assistance au transfert à un autre fournisseur ou à l'organisation elle-même.

Il convient que les organisations établissent et tiennent à jour un registre des accords conclus avec des parties externes (par exemple, contrats, protocoles d'accord, accords de partage d'informations) pour conserver une trace de la destination de leurs informations. Il convient également que les organisations procèdent régulièrement à la revue, la validation et la mise à jour de leurs accords avec des parties externes pour s'assurer que ces accords demeurent nécessaires et sont en adéquation avec les articles pertinents sur la sécurité de l'information.

Informations supplémentaires

Les accords peuvent différer considérablement d'une organisation à l'autre et selon les types de fournisseurs. Il convient donc de veiller à inclure toutes les exigences liées au traitement des risques de sécurité de l'information.

Pour plus de détails sur les accords avec les fournisseurs, voir l'ISO/IEC 27036 (toutes les parties) et, pour les accords relatifs aux services en nuage, voir l'ISO/IEC 19086 (toutes les parties).

5.21 Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient de définir et de mettre en œuvre des processus et procédures destinés à traiter les risques de sécurité de l'information associés aux services de TIC et à la chaîne d'approvisionnement des produits.

Objectif

Garantir la sécurité de l'information de l'organisation dans le cadre de la chaîne d'approvisionnement TIC.

Préconisations

Il convient de prendre en compte les thèmes suivants pour traiter la sécurité de l'information dans le cadre de la sécurité de la chaîne d'approvisionnement TIC, en plus des exigences générales de sécurité de l'information concernant les relations avec les fournisseurs :

a) définir les exigences de sécurité à appliquer à l'acquisition de produits ou de services de TIC ;

b) exiger de la part des fournisseurs de services de TIC qu'ils diffusent les exigences de sécurité de l'organisation jusqu'au dernier maillon de la chaîne d'approvisionnement si le fournisseur sous-traite certaines parties des services de TIC qu'il fournit à l'organisation ;

c) exiger de la part des fournisseurs de produits de TIC qu'ils diffusent les pratiques de sécurité appropriées jusqu'au dernier maillon de la chaîne d'approvisionnement si ces produits sont dotés de composants achetés auprès d'autres fournisseurs ou d'autres entités (par exemple, développeurs de logiciels et fournisseurs de composants matériels externes) ;

d) exiger de la part des fournisseurs de produits de TIC qu'ils fournissent les informations décrivant les composants logiciels utilisés dans les produits ;

e) mettre en œuvre un processus de surveillance et des méthodes acceptables pour valider la conformité des produits et services de TIC avec les exigences de sécurité énoncées ; ces types de méthodes de revue des fournisseurs peuvent, par exemple, comprendre des tests de pénétration et le contrôle ou la validation des attestations de tierce partie portant sur les opérations de sécurité de l'information des fournisseurs ;

f) mettre en œuvre un processus d'identification et de documentation des composants d'un produit ou d'un service critique pour le maintien des fonctionnalités et qui nécessitent, par conséquent, plus d'attention et de soins et un suivi ultérieur lorsqu'ils sont élaborés en dehors de l'organisation, notamment si le fournisseur sous-traite certains aspects des composants du produit ou du service à d'autres fournisseurs ;

g) obtenir l'assurance que les composants critiques et leur origine peuvent être tracés tout au long de la chaîne d'approvisionnement ;

h) obtenir l'assurance que les produits de TIC livrés fonctionnent comme prévu et ne présentent aucune fonctionnalité inattendue ou indésirable ;

i) mettre en œuvre des processus destinés à s'assurer que les composants en provenance des fournisseurs sont authentiques et conformes à leur spécification. Les mesures peuvent, par exemple, correspondre à des étiquettes inviolables, des contrôles de hachage cryptographique ou des signatures numériques. La surveillance des performances non conformes à la spécification peut constituer une indication de fraude ou de contrefaçon ; il convient que la prévention et la détection de fraude soient mises en œuvre en plusieurs étapes au cours du cycle de développement du système, notamment conception, développement, intégration, exploitation et maintenance ;

j) obtenir l'assurance que le produit de TIC atteint les niveaux de sécurité requis, par exemple par le biais d'une certification formelle ou d'un programme d'évaluation tel que l'Arrangement de reconnaissance mutuelle selon les Critères communs ;

k) définir les règles de partage de l'information concernant la chaîne d'approvisionnement et tous les problèmes et compromis possibles entre l'organisation et les fournisseurs ;

l) mettre en œuvre des processus spécifiques de gestion du cycle de vie des composants de TIC et de leur disponibilité, ainsi que des risques de sécurité associés. Cela inclut la gestion des risques présentés par la rupture de stock de composants, les fournisseurs ayant cessé leur activité ou ayant arrêté de produire ces composants en raison des avancées technologiques. Envisager l'identification d'un autre fournisseur et le processus de transfert du logiciel et des compétences à l'autre fournisseur.

Informations supplémentaires

Les pratiques spécifiques de gestion des risques de la chaîne d'approvisionnement TIC consolident les pratiques générales de sécurité de l'information, de qualité, de gestion de projet et d'ingénierie de systèmes, mais ne les remplacent pas.

Il est conseillé aux organisations de travailler avec les fournisseurs pour appréhender la chaîne d'approvisionnement TIC et tous les éléments qui présentent des conséquences importantes sur les produits et les services à fournir. L'organisation peut influer sur les pratiques en matière de sécurité de l'information dans les chaînes d'approvisionnement TIC, en stipulant clairement dans les accords conclus avec les fournisseurs les problèmes qu'il convient que les autres fournisseurs de la chaîne d'approvisionnement TIC résolvent.

Il convient que les produits de TIC soient achetés auprès de sources réputées. La fiabilité des logiciels et du matériel est une question de contrôle qualité. Bien qu'une organisation n'ait généralement pas la possibilité d'inspecter les systèmes de contrôle qualité de ses constructeurs ou éditeurs, elle peut porter un jugement fiable en s'appuyant sur la réputation du constructeur ou éditeur concerné.

La chaîne d'approvisionnement TIC telle qu'elle est traitée ici comprend des services en nuage.

Ci-dessous des exemples de chaînes d'approvisionnement TIC :

a) fourniture de services en nuage, où le fournisseur de services en nuage s'appuie sur des développeurs de logiciels, des fournisseurs de services de télécommunication et des fournisseurs de matériel ;

b) Internet des Objets, où le service fait intervenir les fabricants de dispositifs, les fournisseurs de services en nuage (en l'occurrence l'opérateur de la plateforme d'Internet des Objets), les développeurs d'applications Web et mobiles et l'éditeur de bibliothèques logicielles ;

c) services d'hébergement, où le fournisseur s'appuie sur des centres de services externes et sur le support de premier, deuxième et troisième niveau.

Voir l'ISO/IEC 27036-3 pour de plus amples informations sur les recommandations relatives à l'appréciation du risque.

Les étiquettes d'identification logicielle (SWID) peuvent également contribuer à renforcer la sécurité de l'information dans la chaîne d'approvisionnement, en apportant des informations sur la provenance du logiciel et, le cas échéant, en prenant en charge des mesures de sécurité basées sur les listes d'autorisation et pas uniquement les listes de blocage. Voir l'ISO/IEC 19770-2 pour de plus amples informations.

5.22 Suivi, revue et gestion des changements des services fournisseurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection #Défense

Mesure de sécurité

Il convient que l'organisation procède régulièrement à la surveillance, à la revue, à l'évaluation et à la gestion des changements de pratiques du fournisseur en matière de sécurité de l'information et de prestation de services.

Objectif

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

Préconisations

Il convient que la surveillance, la revue et la gestion des changements des services fournisseurs garantissent que les conditions générales sur la sécurité de l'information prévues dans les accords sont respectées ; que les incidents et les problèmes liés à la sécurité de l'information sont gérés correctement ; et que les changements intervenus dans les services fournisseurs ou la situation de l'entreprise ne nuisent pas à la prestation de services.

Il convient qu'il existe, à cet effet, un processus de gestion de la relation entre l'organisation et le fournisseur en vue de :

a) surveiller les niveaux de performance des services et vérifier ainsi qu'ils sont conformes aux accords ;

b) surveiller les changements apportés par les fournisseurs, dont :

   1) les améliorations apportées aux services proposés ;

   2) le développement de nouvelles applications et de nouveaux systèmes ;

   3) les changements ou les mises à jour des politiques et des procédures du fournisseur ;

   4) les mesures nouvelles ou modifiées permettant de résoudre les incidents liés à la sécurité de l'information et de renforcer la sécurité ;

c) surveiller les changements dans les services assurés par les fournisseurs, dont :

   1) les changements et les améliorations liés aux réseaux ;

   2) l'utilisation de nouvelles technologies ;

   3) l'adoption de nouveaux produits ou de versions plus récentes ;

   4) les nouveaux outils et environnements de développement ;

   5) les changements apportés à l'emplacement physique des équipements de dépannage ;

   6) les changements de sous-traitants ;

   7) la sous-traitance à un autre fournisseur.

d) passer en revue les rapports de service produits par le fournisseur et organiser des réunions régulières sur l'avancement conformément aux termes des accords ;

e) mener des audits des fournisseurs et des sous-traitants conjointement avec la revue de rapports d'audit indépendants, s'ils existent, et assurer le suivi des problèmes identifiés ;

f) fournir les informations relatives aux incidents liés à la sécurité de l'information et assurer une revue de ces informations conformément aux termes des accords et à toutes les lignes directrices et procédures d'accompagnement ;

g) passer en revue les systèmes de traçabilité et les enregistrements du fournisseur concernant les événements de sécurité de l'information, les problèmes d'exploitation, les défaillances et le suivi des pannes et des interruptions liées au service fourni ;

h) répondre aux événements ou incidents liés à la sécurité de l'information identifiés, le cas échéant, et les gérer ;

i) identifier les vulnérabilités liées à la sécurité de l'information et les gérer ;

j) passer en revue les aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs ;

k) s'assurer que le fournisseur maintient une capacité de service suffisante ainsi que des plans exploitables dans le but de garantir le maintien du niveau de continuité de service convenu en cas de défaillance majeure du service ou de sinistre (voir 5.29, 5.35, 5.36, 8.14) ;

l) s'assurer que les fournisseurs nomment les personnes chargées de contrôler le respect et l'application des exigences stipulées dans les accords ;

m) évaluer régulièrement le maintien par les fournisseurs des niveaux de sécurité adéquats.

Il convient d'attribuer la responsabilité de la gestion des relations avec les fournisseurs à une personne ou à une équipe désignée. Il convient de prévoir les compétences et ressources techniques suffisantes pour veiller à ce que les exigences du contrat, et en particulier celles qui traitent de la sécurité de l'information, sont respectées. Il convient de prendre les mesures adéquates lorsque des insuffisances sont observées dans la prestation du service.

Informations supplémentaires

Voir l'ISO/IEC 27036-3 pour de plus amples informations.

5.23 Sécurité de l'information dans l'utilisation de services en nuage

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient que les processus d'acquisition, d'utilisation, de management et de cessation des services en nuage soient définis conformément aux exigences de sécurité de l'information de l'organisation.

Objectif

Spécifier et gérer la sécurité de l'information concernant l'utilisation des services en nuage.

Préconisations

Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème de l'utilisation des services en nuage.

Il convient que l'organisation définisse et communique la façon dont elle entend gérer les risques de sécurité associés aux services en nuage. Il peut s'agir d'une extension ou d'une partie de l'approche existante appliquée par l'organisation pour la gestion des prestations de services externalisées (voir 5.21 et 5.22).

L'utilisation de services en nuage implique un partage des responsabilités liées à la sécurité de l'information et de la collaboration entre le fournisseur de services en nuage et l'organisation qui représente le client des services en nuage. Il est essentiel que les responsabilités qui incombent au fournisseur de services en nuage et à son client soient correctement définies et mises en œuvre.

Il convient que l'organisation définisse :

a) toutes les exigences de sécurité de l'information associées à l'utilisation des services en nuage ;

b) les critères de sélection des services en nuage et le périmètre d'utilisation des services en nuage ;

c) les rôles et responsabilités associés à l'utilisation et au management des services en nuage ;

d) la façon d'obtenir et d'exploiter la sécurité de l'information proposée par le fournisseur de services en nuage ;

e) la façon d'obtenir une assurance quant aux mesures de sécurité de l'information mises en œuvre par le fournisseur de services en nuage ;

f) les modalités de changement ou d'arrêt de l'utilisation des services en nuage, y compris une stratégie de désengagement desdits services ;

g) son approche de surveillance, de revue et d'évaluation de l'utilisation continue des services en nuage pour gérer les risques de sécurité de l'information ;

h) la nature des mesures de sécurité de l'information gérées par le fournisseur de services en nuage et de celles gérées par l'organisation en sa qualité de client des services en nuage ;

i) les procédures de prise en charge des incidents liés à la sécurité de l'information survenus dans le cadre de l'utilisation des services en nuage ;

j) la façon de gérer les mesures, les interfaces et les changements liés aux services lorsqu'une organisation utilise plusieurs services en nuage, notamment s'ils sont assurés par plusieurs fournisseurs de services en nuage.

Pour tous les services en nuage, il convient que l'organisation procède à la revue et à la négociation des accords relatifs aux services en nuage avec le ou les fournisseurs de services en nuage. Il convient qu'un contrat de services en nuage tienne compte des exigences de l'organisation en termes de confidentialité, d'intégrité, de disponibilité et de traitement des DCP, idéalement avec des objectifs de niveau de service et des objectifs qualitatifs concernant les services en nuage. Dans le cas d'un contrat de services en nuage prédéfini et ne pouvant donc faire l'objet d'aucune négociation, il convient que les éventuels risques résiduels soient clairement définis et acceptés par le niveau de direction approprié de l'organisation.

Il convient qu'un contrat conclu entre un fournisseur de services en nuage et un client de services en nuage comprenne les dispositions suivantes en matière de protection des données du client des services en nuage et de disponibilité des services :

a) mise à disposition de solutions basées sur les normes acceptées de l'industrie concernant l'architecture et l'infrastructure ;

b) gestion des contrôles d'accès relatifs aux services en nuage conforme aux exigences de l'organisation ;

c) mise en œuvre de solutions de surveillance et de protection contre les programmes malveillants ;

d) traitement et stockage de l'information sensible de l'organisation dans les lieux approuvés (par exemple, un pays ou une région donné) ou au sein ou sous la responsabilité d'une juridiction particulière ;

e) disponibilité d'un support dédié en cas d'incident de sécurité dans l'environnement des services en nuage ;

f) assurance que les exigences de sécurité de l'organisation seront respectées si les services en nuage sont eux-mêmes sous-traités à un fournisseur externe (ou interdiction de sous-traiter les services en nuage) ;

g) assistance de l'organisation dans le rassemblement de preuves numériques (par exemple, en cas d'action en justice) ;

h) mise à disposition du support et de la disponibilité des services pertinents pendant la période appropriée lorsque l'organisation souhaite arrêter d'utiliser les services en nuage ;

i) sauvegarde des données et des informations de configuration et gestion sécurisée des sauvegardes ;

j) fourniture et restitution de l'information, notamment les fichiers de configuration, le code source et les données qui sont détenues par le client de services en nuage sur demande au cours de la prestation de service ou lors de la résiliation du service.

Il convient que le client de services en nuage considère s'il convient que l'accord exige de la part des fournisseurs de services en nuage qu'ils envoient une notification préalable avant tout changement ayant de lourdes conséquences pour le client, quant aux modalités de mise à disposition du service à l'organisation, notamment :

a) changements apportés à l'infrastructure technique (par exemple, déplacement, reconfiguration ou changements de nature matérielle ou logicielle) qui ont des répercussions ou entraînent une modification de l'offre de services en nuage ;

b) traitement ou stockage de l'information dans une nouvelle zone géographique ou juridiction légale ;

c) recours à d'autres fournisseurs de services en nuage ou à d'autres sous-traitants (y compris changement des intervenants existants ou recours à de nouveaux intervenants).

Il convient que l'organisation qui utilise les services en nuage maintienne un contact étroit avec ses fournisseurs de services en nuage. Ces contacts permettent un échange mutuel d'informations relatives à la sécurité de l'information pour l'utilisation des services en nuage, avec un mécanisme qui permette au fournisseur de services en nuage, mais aussi au client des services en nuage de surveiller chaque caractéristique des services et de signaler les cas de non-respect des engagements contenus dans les accords.

Informations supplémentaires

Cette mesure envisage la sécurité dans le nuage du point de vue du client. Un modèle de déploiement d'informatique en nuage présente l'environnement requis pour organiser le pilotage et la distribution des ressources physiques ou virtuelles. Chacun des modèles de déploiement d'informatique en nuage suivants présente des avantages différents quant à l'utilisation des services en nuage :

a) nuage privé : les services en nuage sont utilisés exclusivement par un client et les ressources sont gérées par ledit client des services en nuage. Le nuage privé peut être détenu et exploité par l'organisation elle-même ou par un fournisseur de services en nuage. Il peut exister sur site ou hors site. Les nuages privés, de par leur nature, n'atteignent habituellement pas l'évolutivité et l'élasticité complètes qu'offrent les services en nuage publics de grande envergure ;

b) nuage public : les services en nuage sont disponibles à tout client de services en nuage et le fournisseur de services en nuage pilote les ressources ;

c) nuage communautaire : les services en nuage sont partagés de façon exclusive par un ensemble de clients de services en nuage ;

d) nuage hybride : deux modèles de déploiement différents sont utilisés.

Les types de services en nuage décrivent les fonctionnalités mises à disposition par un service en nuage, et sont les suivants :

a) type de services applicatifs (SaaS) : le client peut utiliser les applications du fournisseur de services en nuage ;

b) type de services d'infrastructure (IaaS) : le client peut mettre en service et utiliser les ressources de traitement, de stockage ou réseau ;

c) type de services de plateforme (PaaS) : le client peut déployer, gérer et exploiter les logiciels qu'il a créés ou acquis dans un ou plusieurs environnements d'exécution logicielle pris en charge par le fournisseur de services en nuage.

Dans certains cas, si l'organisation souhaite utiliser un service en nuage, la seule option qui s'offre à elle consiste à accepter des conditions de service génériques lors de l'utilisation de certains services en nuage, auquel cas elle ne peut pas négocier un accord de services en nuage qui tienne compte des politiques ou exigences de l'organisation. Dans ce type de scénario, il convient que l'organisation réalise l'appréciation du risque qui en relève afin d'identifier les risques associés à l'utilisation desdits services et gère les risques pendant la durée de l'accord.

Des informations complémentaires sur les services en nuage sont disponibles dans l'ISO/IEC 17788 et dans l'ISO/IEC 17789. Les spécificités liées à la portabilité de l'informatique en nuage en appui des stratégies de désengagement sont disponibles dans l'ISO/IEC 19941. Les spécificités liées à la sécurité de l'information et aux services en nuage publics sont décrites dans l'ISO/IEC 27017. Les relations avec les fournisseurs dans le cadre des services en nuage sont traitées dans l'ISO/IEC 27036-4 et les accords relatifs aux services en nuage et à leur contenu sont traités dans l'ISO/IEC 19086 (toutes les parties), la sécurité et la confidentialité étant traitées de façon spécifique dans l'ISO/IEC 19086-4.

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

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient que l'organisation planifie et prépare la gestion des incidents liés à la sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, rôles et responsabilités dans le cadre de la gestion des incidents liés à la sécurité de l'information.

Objectif

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

Préconisations

Rôles et responsabilités

Il convient que l'organisation établisse une capacité de gestion des incidents liés à la sécurité de l'information à un niveau suffisant. Il convient que les rôles et responsabilités d'exécution des procédures de gestion des incidents soient déterminées et correctement communiquées aux parties intéressées internes et externes pertinentes.

Il convient de considérer les éléments suivants :

a) il convient d'établir une méthode commune de signalement des événements liés à la sécurité de l'information, notamment un point de contact (voir 6.8) ;

b) il convient de constituer une équipe de réponse aux incidents (IRT) pour donner à l'organisation la faculté d'apprécier les incidents liés à la sécurité de l'information, d'y répondre et d'en tirer des enseignements ;

c) il convient que seul le personnel compétent au sein de l'organisation traite les questions relatives aux incidents liés à la sécurité de l'information. Il convient que ce personnel dispose de la documentation relative aux procédures et qu'il bénéficie d'une formation régulière ;

d) il convient d'établir un processus destiné à identifier les besoins en formation, en certification et en formation continue du personnel chargé de la réponse aux incidents.

Procédures de gestion des incidents

Il convient que les objectifs de la gestion des incidents liés à la sécurité de l'information fassent l'objet d'un accord avec la direction. Il convient également de s'assurer que les personnes responsables de la gestion des incidents liés à la sécurité de l'information connaissent les priorités de l'organisation dans ce domaine, notamment les délais de résolution en fonction de l'impact potentiel et de la gravité. Il convient de mettre en œuvre des procédures de gestion des incidents pour satisfaire à ces objectifs et priorités.

Il convient que la direction s'assure qu'un plan de gestion des incidents liés à la sécurité de l'information soit créé en envisageant l'élaboration et la mise en œuvre de plusieurs scénarios et procédures pour les activités suivantes :

a) évaluation des événements liés à la sécurité de l'information en fonction de critères permettant de déterminer ce qui constitue un incident lié à la sécurité de l'information ;

b) surveillance (voir 8.14 et 8.15), détection (voir 8.15), classification (voir 5.25), analyse et reporting (voir 6.8) des événements et incidents liés à la sécurité de l'information (par des moyens humains ou automatiques) ;

c) gestion des incidents liés à la sécurité de l'information jusqu'à leur terme, y compris réponse et remontée d'information (voir 5.26), en fonction du type et de la catégorie de l'incident, activation éventuelle d'une gestion de crise et de plans de continuité, récupération contrôlée de l'incident et communication aux parties intéressées internes et externes ;

d) coordination avec les parties intéressées internes et externes, telles que le conseil, les autorités, les groupes d'intérêt externes et les forums, fournisseurs et clients (voir 5.5 et 5.6) ;

e) journalisation des activités de gestion des incidents ;

f) prise en charge des preuves numériques (voir 5.28) ;

g) procédures d'analyse des causes profondes ou d'analyse rétrospective ;

h) identification des enseignements tirés et des améliorations éventuelles des procédures de gestion des incidents ou des mesures de sécurité de l'information qui s'avèrent nécessaires d'un point de vue général.

Procédures de signalement

Il convient que les procédures de signalement prévoient :

a) les actions à engager lorsqu'un événement lié à la sécurité de l'information se produit (à savoir, noter immédiatement tous les détails pertinents, par exemple la défaillance et les messages apparaissant à l'écran, en informer immédiatement le responsable servant de point de contact et n'exécuter que des actions concertées) ;

b) l'utilisation de formulaires d'incidents pour aider le personnel à effectuer toutes les actions nécessaires lors du signalement d'incidents liés à la sécurité de l'information ;

c) des processus de retour d'information adéquats, afin de communiquer, dans la mesure du possible, les détails de la résolution du problème aux personnes ayant signalé un événement, une fois que le problème a été réglé et clôturé ;

d) création de rendus d'incidents.

Il convient de prendre en compte les éventuelles exigences extérieures quant au signalement des incidents aux parties intéressées pertinentes dans le délai prévu (par exemple, exigences de notification des violations aux régulateurs) lors de la mise en œuvre des procédures de gestion des incidents.

Informations supplémentaires

Un événement lié à la sécurité de l'information est une occurrence qui indique une possible violation de la sécurité de l'information ou une défaillance des mesures. Un incident lié à la sécurité de l'information correspond à un ou plusieurs événements liés à la sécurité de l'information, qui répondent aux critères définis et peuvent porter préjudice aux actifs de l'organisation ou compromettre son fonctionnement

Les incidents liés à la sécurité de l'information peuvent dépasser les frontières de l'organisation et du pays. Pour traiter les incidents de ce type, il est judicieux de coordonner les réponses et de partager les informations relatives à ces incidents avec les autres organisations s'il y a lieu.

L'ISO/IEC 27035 (toutes les parties) fournit des recommandations détaillées relatives à la gestion des incidents liés à la sécurité de l'information.

5.25 Appréciation des événements liés à la sécurité de l'information et prise de décision

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient que l'organisation apprécie les événements liés à la sécurité de l'information et qu'elle décide s'ils doivent être classés dans la catégorie des incidents liés à la sécurité de l'information.

Objectif

Classer les événements liés à la sécurité de l'information dans la catégorie appropriée et leur attribuer la priorité correcte.

Préconisations

Il convient de définir un plan de catégorisation et de priorisation des incidents en vue de l'identification de l'impact et de la priorité de chaque incident. Il convient que le plan inclue les critères permettant de classer les événements dans la catégorie des incidents liés à la sécurité de l'information. Il convient que le point de contact apprécie chaque événement lié à la sécurité de l'information à l'aide du plan défini.

Il convient que le personnel chargé de la coordination et de la réponse aux incidents liés à la sécurité de l'information procède à l'appréciation des événements liés à la sécurité de l'information et qu'il prenne une décision les concernant.

Il convient d'enregistrer les conclusions de l'appréciation et la décision de manière détaillée en vue de contrôles ou de références ultérieurs.

Informations supplémentaires

L'ISO/IEC 27035 (toutes les parties) donne des recommandations supplémentaires sur la gestion des incidents.

5.26 Réponse aux incidents liés à la sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient de répondre aux incidents liés à la sécurité de l'information conformément aux procédures documentées.

Objectif

Apporter une réponse efficace aux incidents liés à la sécurité de l'information.

Préconisations

Il convient que l'organisation établisse des procédures de réponse aux incidents et qu'elle les communique à toutes les parties intéressées.

Il convient que les incidents liés à la sécurité de l'information soient traités par une équipe désignée dotée des compétences requises (voir 5.24).

Il convient que la réponse comporte :

a) l'indication, si l'impact de l'incident peut s'étendre, des systèmes impactés par l'incident ;

b) le recueil de preuves aussitôt que possible après l'incident ;

c) une remontée d'informations avec, le cas échéant, des activités de gestion de crise et le recours à des plans de continuité d'activité (voir 5.29 et 5.30) ;

d) l'assurance que toutes les tâches concernant la réponse sont correctement journalisées en vue d'une analyse ultérieure ;

e) la communication de l'existence d'un incident lié à la sécurité de l'information ou de tout détail pertinent qui s'y rapporte aux autres personnes ou organisations internes et externes en suivant le principe du besoin d'en connaître ;

f) la coordination avec les personnes ou organisations internes et externes, dont les autorités, les groupes d'intérêt externes ou les forums pour améliorer l'efficacité des réponses et réduire au minimum l'impact sur les autres organisations ;

g) une fois que l'incident a été résolu avec succès, la clôture formelle de l'incident et son enregistrement ;

h) une analyse scientifique de la sécurité de l'information, le cas échéant (voir 5.28) ;

i) une analyse post-incident pour identifier la cause profonde. Veiller à ce qu'elle soit documentée et communiquée suivant les procédures définies (voir 5.27) ;

j) l'identification et la gestion des vulnérabilités et points faibles en matière de sécurité de l'information, y compris ceux qui concernent les mesures qui ont provoqué l'incident, ont contribué à ce qu'il survienne ou n'ont pas permis de le prévenir.

Informations supplémentaires

De façon générale, le principal objectif de la réponse aux incidents liés à la sécurité de l'information est de rétablir le fonctionnement normal de l'activité et du système d'information avec les niveaux de sécurité requis puis de lancer de nouvelles activités de récupération.

L'ISO/IEC 27035 (toutes les parties) donne des recommandations supplémentaires sur la gestion des incidents.

5.27 Tirer des enseignements des incidents liés à la sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection #Identification	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient de tirer profit des connaissances acquises à partir des incidents liés à la sécurité de l'information pour renforcer et améliorer l'environnement de contrôle.

Objectif

Réduire la probabilité ou les conséquences d'incidents ultérieurs.

Préconisations

Il convient que l'organisation établisse des procédures pour quantifier et surveiller les types, le volume et le coût des incidents liés à la sécurité de l'information. Il convient de se servir des informations recueillies lors de l'évaluation de ces incidents pour identifier les incidents récurrents ou ayant des conséquences graves, afin de planifier et de mettre en œuvre des changements visant à réduire la probabilité ou les conséquences d'incidents similaires à l'avenir.

Il convient de se servir des informations recueillies lors de l'évaluation des incidents liés à la sécurité de l'information pour :

a) enrichir le plan de gestion des incidents, notamment les scénarios et procédures relatifs aux incidents (voir 5.24) ;

b) identifier les incidents récurrents ou ayant de graves conséquences et leur cause pour mettre à jour l'appréciation du risque de sécurité de l'information, et déterminer et mettre en œuvre les mesures de sécurité supplémentaires qui s'avèrent nécessaires pour réduire la probabilité ou les conséquences d'incidents similaires à l'avenir. Activer des mécanismes tels que le recueil, la quantification et la surveillance des informations relatives aux types d'incidents, à leur volume et à leur coût ;

c) enrichir le programme de sensibilisation des utilisateurs (voir 6.3) avec des exemples de situations susceptibles de se produire, le mode de traitement des incidents de ce type et les procédures à mettre en place pour éviter leur réapparition.

Informations supplémentaires

L'ISO/IEC 27035 (toutes les parties) donne des recommandations supplémentaires.

5.28 Recueil de preuves

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient que l'organisation établisse et mette en œuvre des procédures d'identification, de recueil, d'acquisition et de protection de l'information à partir des incidents liés à la sécurité de l'information.

Objectif

Assurer une gestion cohérente et efficace des preuves relatives aux incidents liés à la sécurité de l'information dans le cadre d'une action judiciaire ou d'une mesure disciplinaire.

Préconisations

Il convient de mettre au point et d'appliquer des procédures internes de traitement des preuves dans le cadre d'une action judiciaire ou d'une mesure disciplinaire. Il convient de tenir compte des exigences des diverses juridictions afin d'optimiser l'admissibilité de la preuve auprès des juridictions compétentes.

Il convient, en général, que les procédures relatives à la gestion des preuves prévoient des instructions d'identification, de recueil, d'acquisition et de protection selon les différents types de supports, de dispositifs et d'état des dispositifs, par exemple allumé ou éteint. Les preuves doivent généralement être recueillies d'une manière admise par les tribunaux nationaux compétents ou autres instances disciplinaires. Il convient de pouvoir montrer que :

a) les enregistrements sont complets et n'ont en aucune façon été falsifiés ;

b) les copies des preuves numériques sont en tous points identiques aux originaux ;

c) le système informatique dont la preuve est issue fonctionnait correctement lors de l'enregistrement de la preuve.

S'il en existe, il convient de rechercher les certifications et autres justificatifs de la qualification du personnel et des outils, de sorte à renforcer la valeur des preuves protégées.

Les preuves numériques peuvent dépasser les limites de l'organisation ou les frontières juridictionnelles. Dans ce cas, il convient de s'assurer que l'organisation est habilitée à recueillir les informations devant servir de preuve numérique.

Informations supplémentaires

L'identification est le processus impliqué dans la recherche, la reconnaissance et la documentation de preuves potentielles. Le recueil de preuves est le processus consistant à rassembler des éléments physiques pouvant contenir des preuves potentielles. L'acquisition est le processus de création d'une copie des données considérée comme ayant valeur de preuve à l'égard de l'événement soumis à investigation. La protection est le processus consistant à maintenir et sauvegarder l'intégrité et l'état d'origine des preuves potentielles.

À la première détection d'un événement lié à la sécurité de l'information, il n'est pas toujours possible de prévoir si l'événement fera l'objet d'une action en justice. Les preuves nécessaires risquent donc d'être détruites, volontairement ou non, avant que la gravité de l'incident ne soit avérée. Il est souhaitable de consulter un avocat ou la police rapidement, en vue d'une éventuelle action en justice, afin de recueillir les conseils relatifs à la preuve.

L'ISO/IEC 27037 fournit des lignes directrices concernant l'identification, le recueil, l'acquisition et la protection des preuves numériques.

L'ISO/IEC 27050 (toutes les parties) traite de la découverte électronique, qui implique le traitement d'informations enregistrées électroniquement en tant que preuves.

5.29 Sécurité de l'information durant une perturbation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Continuité	#Protection #Résilience

Mesure de sécurité

Il convient que l'organisation planifie la procédure de maintien de la sécurité de l'information au niveau approprié en cas de perturbation.

Objectif

Assurer la protection adéquate de l'information et des autres actifs associés en cas de perturbation.

Préconisations

Il convient que l'organisation détermine ses exigences pour adapter les mesures de sécurité de l'information en cas de perturbation. Il convient d'intégrer les exigences de sécurité de l'information dans les processus de gestion de la continuité d'activité.

Il convient d'élaborer, de mettre en œuvre, de tester, de réviser et d'évaluer des plans visant à assurer ou rétablir la sécurité de l'information dans les processus métier critiques suite à une interruption ou une défaillance. Il convient de rétablir la sécurité de l'information au niveau et dans les échelles de temps requis.

Il convient que l'organisation mette en œuvre et gère :

a) les mesures de sécurité de l'information, et les systèmes et outils sous-jacents dans les plans de continuité d'activité et de continuité TIC ;

b) des processus pour mettre à jour les mesures de sécurité de l'information existantes en cas de perturbation ;

c) des mesures destinées à contrebalancer les mesures de sécurité de l'information qu'il est impossible de maintenir en cas de perturbation.

Informations supplémentaires

Dans le contexte de la planification de la continuité d'activité et de la continuité des TIC, il peut être nécessaire d'adapter les exigences de sécurité de l'information en fonction du type de perturbation, par rapport aux conditions de fonctionnement normales. Dans le cadre du bilan d'impact sur l'activité et de l'appréciation du risque réalisés pour la gestion de la continuité d'activité, il convient de prendre en compte les conséquences de la perte de confidentialité et d'intégrité de l'information et de leur attribuer une priorité, en plus de la nécessité de maintenir la disponibilité.

Des informations supplémentaires sont disponibles dans l'ISO 22313 et l'ISO 22301.

5.30 Préparation des TIC pour la continuité d'activité

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Protection #Correction	#Disponibilité	#Protection #Traitement	#Continuité	#Résilience

Mesure de sécurité

Il convient de planifier, de mettre en œuvre, de gérer et de tester la préparation des TIC en fonction des objectifs de continuité d'activité et des exigences de continuité des TIC.

Objectif

Assurer la disponibilité de l'information et des autres actifs associés de l'organisation en cas de perturbation.

Préconisations

La préparation des TIC pour la continuité d'activité constitue un élément important dans la gestion de la continuité d'activité et le management de la sécurité de l'information pour garantir que les objectifs de l'organisation pourront continuer à être remplis en cas de perturbation.

Les exigences de continuité des TIC sont produites à partir du bilan d'impact sur l'activité (BIA). Il convient que le processus de BIA utilise les types et les critères d'impact pour apprécier les impacts au fil du temps, qui découlent de la perturbation des activités visant à fournir des produits et des services. Il convient d'utiliser l'importance et la durée de l'impact obtenu pour identifier les activités prioritaires, auxquelles il convient d'attribuer un objectif de délai de reprise (RTO). Il convient ensuite que le BIA détermine les ressources nécessaires pour soutenir les activités prioritaires. Il convient également de préciser un RTO pour ces ressources. Il convient qu'un sous-ensemble de ces ressources comprenne les services de TIC. En collaboration avec le personnel chargé de gérer la continuité d'activité, le bilan d'impact sur l'activité relatif aux services de TIC peut être développé avec les exigences en termes de performances et de capacité des systèmes de TIC, ainsi que les points de récupération des données (RPO) de l'information destinés à soutenir les activités en cas de perturbation.

En se basant sur les éléments de sortie du bilan d'impact sur l'activité et de l'appréciation du risque pour les services de TIC, il convient que l'organisation identifie et sélectionne des stratégies de continuité des TIC qui prennent en compte des options pour les périodes situées avant, pendant et après la perturbation. Les stratégies de continuité d'activité peuvent comprendre une ou plusieurs solutions. Sur la base des stratégies, il convient d'élaborer, de mettre en œuvre et de tester des plans pour respecter le niveau de disponibilité requis des services de TIC et les délais prévus consécutivement à l'interruption ou à la défaillance de processus métier critiques.

Il convient que l'organisation s'assure :

a) qu'il existe une structure organisationnelle adéquate pour se préparer, atténuer et réagir à une perturbation en mobilisant du personnel possédant la responsabilité, l'autorité et les compétences nécessaires ;

b) que les plans de continuité des TIC, y compris les procédures de réponse et de récupération détaillant la façon dont l'organisation gérera une perturbation des services de TIC, sont :

    1) régulièrement évalués par le biais d'exercices et de tests ;

    2) approuvés par la direction ;

c) que les plans de continuité des TIC comprennent les informations de continuité des TIC suivantes :

    1) spécifications de performances et de capacité pour satisfaire aux exigences et objectifs de continuité d'activité tels que spécifiés dans le BIA ;

    2) objectif de délai de reprise (RTO) de chaque composant d'un service de TIC prioritaire et procédures de restauration des composants concernés ;

    3) point de récupération des données (RPO) des ressources de TIC prioritaires définies en tant qu'information et procédures de restauration de l'information concernée.

Informations supplémentaires

La nécessité d'une préparation des TIC pour la continuité d'activité peut résulter des appréciations des risques. L'appréciation doit comprendre tous les types de scénarios, y compris ceux caractérisés par de graves conséquences et une faible probabilité, que l'on qualifie souvent d'extrêmes, mais qui restent plausibles. Une défaillance des services de TIC prioritaires, quelle qu'en soit la raison, aura des conséquences sur la continuité des opérations métier. À ce titre, la gestion de la continuité d'activité constitue une partie essentielle des exigences de continuité d'activité ayant trait à la disponibilité, pour pouvoir :

a) traiter une perturbation des services de TIC, quelle qu'en soit la cause, et se rétablir ;

b) s'assurer que la continuité des activités prioritaires est prise en charge par les services de TIC requis ;

c) répondre avant qu'une perturbation des services de TIC ne survienne, en détectant au moins un incident susceptible d'entraîner une perturbation des services de TIC.

D'autres recommandations sur les procédures TIC sont disponibles dans l'ISO/IEC 27031.

D'autres recommandations sur le système de management de la continuité d'activité sont disponibles dans l'ISO 22301 et l'ISO 22313.

D'autres recommandations sur le bilan d'impact sur l'activité (BIA) sont disponibles dans l'ISO/TS 22317.

5.31 Identification des exigences légales, statutaires, réglementaires et contractuelles

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Législation_et_conformité	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient d'identifier, de documenter et de tenir à jour les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences.

Objectif

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

Préconisations

Généralités

Il convient de prendre en compte les exigences extérieures, notamment d'ordre légal, statutaire, réglementaire ou contractuel, dans les situations suivantes :

a) conception, mise en œuvre ou modification des mesures de sécurité de l'information ;

b) classification de l'information et des autres actifs associés dans le cadre du processus de paramétrage des exigences de sécurité de l'information pour les besoins internes ou dans le cadre d'accords avec les fournisseurs ;

c) réalisation d'appréciations des risques de sécurité de l'information et détermination des activités de traitement des risques de sécurité de l'information ;

d) détermination des processus conjointement avec les rôles et responsabilités correspondants en matière de sécurité de l'information ;

e) détermination des exigences contractuelles des fournisseurs pertinentes pour l'organisation ainsi que du périmètre de fourniture des produits et des services.

Exigences réglementaires et juridiques

Il convient que l'organisation :

a) identifie toutes les législations et réglementations pertinentes pour la sécurité de son information afin de satisfaire aux exigences de son type d'activité ;

b) prenne en compte la conformité dans tous les pays pertinents, si elle :

   1) mène son activité dans d'autres pays ;

   2) utilise des produits et services provenant d'autres pays dans lesquels les lois et réglementations peuvent affecter l'organisation ; ou

   3) transfère des informations au-delà des limites juridictionnelles où les lois et réglementations peuvent affecter l'organisation ;

c) passe régulièrement en revue la législation et les réglementations identifiées de sorte à se tenir informée des changements et à identifier la nouvelle législation ;

d) définisse et documente les différents processus et responsabilités pour satisfaire à ces exigences.

Cryptographie

La cryptographie est un domaine qui comporte souvent des exigences légales spécifiques. En vue de se conformer aux accords, lois et réglementations applicables, il convient de prendre en compte les éléments suivants :

a) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels destinés à l'exécution de fonctions cryptographiques ;

b) les restrictions en matière d'importation ou d'exportation de matériels et de logiciels intégrant des fonctions cryptographiques ;

c) les restrictions en matière d'utilisation de la cryptographie ;

d) les méthodes obligatoires ou discrétionnaires dont disposent les autorités nationales pour accéder aux informations chiffrées ;

e) la validité des signatures, cachets et certificats numériques.

Il convient de demander un avis juridique afin de s'assurer de la conformité aux lois et réglementations en vigueur, en particulier lorsque des informations chiffrées ou des outils de cryptographie sont déplacés au-delà des limites juridictionnelles.

Exigences contractuelles

Il convient que les exigences contractuelles relatives à la sécurité de l'information prennent en compte celles énoncées dans :

a) les contrats avec les clients ;

b) les contrats avec les fournisseurs (voir 5.20) ;

c) les contrats d'assurance.

Informations supplémentaires

Il peut exister des restrictions à l'importation ou à l'exportation de matériel informatique, qui couvrent des questions autres que la cryptographie. Celles-ci ne relèvent pas du domaine d'application du présent document. Un conseil juridique peut s'avérer nécessaire pour identifier l'applicabilité des réglementations et les conséquences potentielles d'une non-conformité.

5.32 Droits de propriété intellectuelle

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Législation_et_conformité	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient que les organisations mettent en œuvre les procédures appropriées pour protéger les droits de propriété intellectuelle.

Objectif

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

Préconisations

Il convient de prendre en compte les lignes directrices suivantes en vue de protéger tout matériel pouvant être soumis à des droits de propriété intellectuelle :

a) publier des procédures relatives aux droits de propriété intellectuelle définissant l'utilisation légale des logiciels et des produits liés à l'information ;

b) acquérir des logiciels uniquement à partir de sources connues et réputées afin de s'assurer du respect des droits d'auteur ;

c) définir et communiquer une politique portant sur le thème de la protection des droits de propriété intellectuelle ;

d) tenir à jour des registres des actifs appropriés et identifier tous les actifs soumis à des exigences de protection des droits de propriété intellectuelle ;

e) conserver les preuves tangibles de la propriété des licences, des disques maîtres, des manuels, etc. ;

f) mettre en œuvre des mesures permettant de s'assurer que le nombre maximal d'utilisateurs ou de ressources (par exemple, CPU) autorisé par la licence n'est pas dépassé ;

g) effectuer des revues permettant de s'assurer que seuls des logiciels autorisés et sous licence sont installés ;

h) mettre en œuvre des procédures de gestion des conditions de licence appropriées ;

i) mettre en œuvre des procédures permettant de céder les logiciels ou de les transmettre à des tiers ;

j) se conformer aux conditions générales régissant les logiciels et l'information obtenus à partir de réseaux publics et de sources extérieures ;

k) ne pas reproduire, convertir dans un autre format ou extraire de l'information à partir d'enregistrements du commerce (vidéo, audio) en dehors de ce qui est permis par la législation sur les droits d'auteur ou les licences en vigueur ;

l) ne pas copier, intégralement ou en partie, des normes (par exemple, normes ISO), livres, articles, rapports ou autres documents, en dehors de ce qui est permis par la législation sur les droits d'auteur ou les licences en vigueur.

Informations supplémentaires

Les droits de propriété intellectuelle incluent les droits d'auteur régissant les logiciels et les documents, les droits des dessins et modèles, les marques, les brevets et les licences régissant le code source.

Les logiciels propriétaires sont généralement dotés d'une licence d'utilisation stipulant les conditions générales de la licence, telles que la limitation de l'utilisation des produits à des ordinateurs spécifiques ou la limitation de la reproduction à la seule création de copies de sauvegarde. Voir l'ISO/IEC 19770 (toutes les parties) pour plus d'informations sur la gestion des actifs logiciels.

Des données peuvent être acquises auprès de sources extérieures. En règle générale, ce type de données est obtenu en vertu des dispositions d'un accord relatif au partage de données ou d'un instrument juridique similaire. Il convient que ce type d'accord relatif au partage de données précise la nature du traitement autorisé pour les données acquises. Il est également recommandé que la provenance des données soit clairement indiquée. Voir l'ISO/IEC 23751 pour plus d'informations sur les accords relatifs au partage de données.

Les exigences légales, statutaires, réglementaires et contractuelles peuvent restreindre la copie du matériel propriétaire. Les exigences applicables peuvent notamment stipuler que seul un matériel développé par l'organisation ou un matériel pour lequel l'organisation dispose de licences, ou encore qui est fourni par un développeur à l'organisation, peut être utilisé. La violation des droits d'auteur peut déclencher une action judiciaire pouvant aboutir à des poursuites pénales.

5.33 Protection des enregistrements

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Législation_et_conformité #Gestion_des_actifs #Protection_des_informations	#Défense

Mesure de sécurité

Il convient de protéger les enregistrements de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées conformément aux exigences légales, statutaires, réglementaires, contractuelles et aux exigences métier.

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires ou contractuelles liées à la protection des enregistrements.

Préconisations

Au moment de décider de la protection spécifique des enregistrements de l'organisation, il convient de tenir compte de leur classification en termes de sécurité de l'information, proposée par le plan de classification de l'organisation. Il convient de classer les enregistrements par types, tels que documents comptables, enregistrements de base de données, journaux de transactions, journaux de modification et procédures d'exploitation ; chaque type comporte des détails sur les périodes de conservation et le type de support de stockage autorisé, par exemple papier, microfiche, support magnétique, support optique. Il convient également de stocker les clés cryptographiques qui s'y rapportent et les programmes associés à des archives ou des signatures électroniques chiffrées (voir 8.24), afin de permettre le déchiffrement des enregistrements pendant leur durée de conservation.

Il convient d'envisager l'éventualité d'une dégradation du support utilisé pour le stockage des enregistrements.

Il convient de mettre en œuvre les procédures de stockage et de manipulation conformément aux recommandations du fabricant des supports de stockage.

Si le choix se porte sur des supports de stockage électroniques, il convient d'établir des procédures visant à garantir l'accès aux données (lisibilité du support et du format) tout au long de la période de conservation afin de protéger les données contre toute perte due à l'évolution de la technologie.

Il convient de choisir les systèmes de stockage des données de sorte qu'ils permettent la récupération des données requises dans un délai raisonnable et sous un format lisible selon les exigences à respecter.

Il convient que le système de stockage et de manipulation garantisse l'identification des enregistrements et de leur durée de conservation telles que définies par la législation nationale ou régionale ou par les réglementations, le cas échéant. Il convient que ce système permette la destruction appropriée des enregistrements à l'issue de cette période si l'organisation n'en a plus besoin.

Pour remplir ces objectifs de sauvegarde des enregistrements, il convient que l'organisation suive les étapes suivantes :

a) il convient d'établir des lignes directrices relatives au stockage, à la manipulation et à l'élimination des enregistrements et de l'information, ce qui inclut l'interdiction de manipuler les données ou enregistrements ;

b) il convient d'établir un programme de conservation définissant les enregistrements et leur durée de conservation.

Informations supplémentaires

Certains enregistrements peuvent nécessiter une conservation sécurisée afin de satisfaire aux exigences légales, statutaires, réglementaires ou contractuelles et de soutenir les activités essentielles de l'organisation. Il peut s'agir d'enregistrements pouvant être requis dans le but de prouver qu'une organisation se conforme aux règles légales, statutaires ou réglementaires, d'assurer une défense dans le cadre d'une action civile ou pénale éventuelle ou de confirmer la situation financière d'une organisation auprès de parties intéressées. La réglementation ou la loi du pays peuvent déterminer la période de conservation de l'information, ainsi que son contenu. D'autres informations sur la gestion des enregistrements sont disponibles dans l'ISO 15489.

5.34 Vie privée et protection des DCP

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Protection_des_informations #Législation_et_conformité	#Protection

Mesure de sécurité

Il convient que l'organisation identifie et satisfasse aux exigences en termes de protection de la vie privée et des DCP conformément aux lois, réglementations et exigences contractuelles en vigueur.

Objectif

Assurer la conformité aux exigences légales, statutaires, réglementaires ou contractuelles liées aux aspects de la sécurité de l'information portant sur la protection des données à caractère personnel (DCP).

Préconisations

Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème de la confidentialité et de la protection des DCP.

Il convient que l'organisation élabore et mette en œuvre des procédures permettant de protéger la vie privée et les DCP. Il convient de communiquer ces procédures à toutes les parties impliquées dans le traitement des données à caractère personnel.

La conformité à ces procédures et à toutes les législations et réglementations pertinentes en matière de protection de la vie privée et des données à caractère personnel exige des rôles, des responsabilités et des mesures de sécurité appropriés. La meilleure façon de mettre en place une telle structure est de désigner un responsable, par exemple un administrateur de la protection de la vie privée. Il convient que cet administrateur conseille le personnel, les fournisseurs de services et les autres parties intéressées sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de respecter.

Il convient que la responsabilité du traitement des DCP soit assumée conformément à la législation et aux réglementations en vigueur.

Il convient de mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel.

Informations supplémentaires

De nombreux pays ont introduit une législation imposant des contrôles sur la collecte, le traitement, la transmission et la suppression des DCP (il s'agit généralement de données sur des personnes en vie, pouvant être identifiées à partir de cette information). Selon la législation nationale concernée, ces contrôles peuvent imposer des obligations à ceux qui recueillent, traitent et diffusent des DCP ; en outre, ces contrôles peuvent imposer des restrictions sur la possibilité de transférer ces données vers d'autres pays.

L'ISO/IEC 29100 propose un cadre général pour la protection des DCP au sein des systèmes de TIC. D'autres informations sur le management de la protection de la vie privée sont disponibles dans l'ISO/IEC 27701. Des informations spécifiques sur le management de la protection de la vie privée dans l'informatique en nuage public agissant comme processeur de DCP sont disponibles dans l'ISO/IEC 27018.

L'ISO/IEC 29134 propose des lignes directrices pour l'évaluation de l'impact sur la vie privée (PIA) ainsi que la structure idéale et le contenu d'un rapport PIA. Par rapport à l'ISO/IEC 27005, celle-ci est axée sur le traitement des DCP et intéresse les organismes qui traitent des données à caractère personnel. Elle peut aider à identifier les risques pour la vie privée et les atténuations possibles pour ramener ces risques à des niveaux acceptables.

5.35 Revue indépendante de la sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Identification	#Assurance_de_sécurité_de_l'information	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de procéder à des revues indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information, y compris des personnes, processus et technologies, à intervalles définis ou lorsque des changements importants sont intervenus.

Objectif

Veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche de l'organisation en matière de management de la sécurité de l'information.

Préconisations

Il convient que l'organisation dispose de processus permettant de mener des revues indépendantes.

Il convient que la direction planifie et lance des revues indépendantes périodiques. Il convient que les revues permettent d'analyser les opportunités d'amélioration et les changements éventuels à apporter à l'approche adoptée en matière de sécurité de l'information, en particulier à la politique, aux politiques portant sur des thèmes et aux mesures.

Il convient que lesdites revues soient réalisées par des personnes indépendantes du domaine concerné, par exemple par des intervenants de la fonction d'audit interne, par un gestionnaire indépendant ou un organisme tiers spécialisé dans ce type de revues. Il convient que les personnes chargées de ces revues possèdent les compétences nécessaires. Il convient que la personne qui mène les revues n'appartienne pas à la structure hiérarchique et qu'elle dispose ainsi de l'indépendance nécessaire pour effectuer une analyse.

Il convient de communiquer les résultats des revues indépendantes à la direction à l'origine de la demande et, le cas échéant, à la direction générale. Il convient de conserver ces enregistrements.

Si les revues indépendantes déterminent que l'approche de l'organisation et sa mise en œuvre du management de la sécurité de l'information sont inadaptés, à savoir que les objectifs et les exigences documentés ne sont pas respectés ou ne sont pas conformes aux directives énoncées dans la politique de sécurité de l'information et les politiques portant sur des thèmes (voir 5.1), il convient que la direction déclenche des actions correctives.

Outre les revues indépendantes périodiques, il convient que l'organisation envisage de mener des revues indépendantes lorsque :

a) les lois et réglementations qui la concernent évoluent ;

b) des incidents importants se produisent ;

c) l'organisation débute une nouvelle activité ou fait évoluer une activité existante ;

d) l'organisation commence à utiliser un nouveau produit ou service, ou apporte des changements à l'utilisation d'un produit ou service actuel ;

e) l'organisation apporte d'importants changements à ses mesures et procédures de sécurité de l'information.

Informations supplémentaires

L'ISO/IEC 27007 et l'ISO/IEC TS 27008 propose des recommandations relatives à la réalisation de revues indépendantes.

5.36 Conformité aux politiques et normes de sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Législation_et_conformité	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de vérifier régulièrement la conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux normes de l'organisation.

Objectif

Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques organisationnelles, aux politiques portant sur des thèmes et aux normes.

Préconisations

Il convient que les responsables et les propriétaires de produits ou services déterminent la manière de vérifier que les exigences de sécurité de l'information définies dans les politiques, les normes et autres réglementations applicables, sont respectées. Il convient d'envisager l'utilisation d'outils de mesure et d'enregistrement automatisés pour procéder à des revues régulières efficaces.

Si la revue détecte une non-conformité, il convient que les responsables :

a) déterminent les causes de la non-conformité ;

b) évaluent la nécessité d'engager des actions correctives pour établir la conformité ;

c) mettent en œuvre les actions correctives appropriées ;

d) vérifient les actions correctives entreprises pour s'assurer de leur efficacité et identifier les insuffisances ou failles éventuelles.

Il convient que les résultats des revues et des actions correctives réalisées par les responsables et les propriétaires de produits ou services soient enregistrés et que ces enregistrements soient tenus à jour. Il convient que ces résultats soient communiqués aux personnes réalisant des revues indépendantes (voir 5.35) par le responsable concerné lorsqu'une revue indépendante est menée dans son domaine de responsabilité.

Il convient que les actions correctives soient réalisées dans les meilleurs délais compte tenu du risque. Si elles ne sont pas achevées à la prochaine revue planifiée, il convient au moins de traiter l'avancement lors de cette revue.

Informations supplémentaires

La surveillance de l'exploitation du système est abordée en 8.16, 8.15, 8.17.

5.37 Procédures d'exploitation documentées

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Disponibilité #Confidentialité #Intégrité	#Protection	#Continuité #Gestion_des_actifs #Sécurité_physique #Sécurité_système_et_réseau	#Gouvernance_et_écosystème #Protection #Défense

Mesure de sécurité

Il convient de documenter les procédures d'exploitation relatives aux moyens de traitement de l'information et de les mettre à disposition de tout le personnel concerné.

Objectif

S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

Préconisations

Il convient d'élaborer des procédures documentées pour les activités opérationnelles de l'organisation associées à la sécurité de l'information, par exemple dans les cas suivants :

a) il convient que l'activité soit effectuée de la même façon par plusieurs personnes ;

b) l'activité est rarement effectuée, de sorte que la procédure risque d'avoir été oubliée lors de l'exécution suivante ;

c) il s'agit d'une nouvelle activité qui présente un risque si elle n'est pas effectuée correctement.

d) Il convient que les procédures d'exploitation spécifient :

e) les personnes responsables ;

f) l'installation sécurisée et la configuration des systèmes ;

g) le traitement et la manipulation de l'information, qu'ils soient automatisés ou manuels ;

h) la sauvegarde (voir 8.13) et la résilience ;

i) les exigences en matière de programmation, notamment les interdépendances avec d'autres systèmes ;

j) les instructions pour gérer les erreurs ou autres conditions exceptionnelles (par exemple, les restrictions liées à l'utilisation des programmes utilitaires (voir 8.18)), susceptibles de survenir lors de l'exécution de la tâche ;

k) les relations avec l'assistance technique et la hiérarchie, y compris les relations avec l'assistance technique externe, en cas de difficultés techniques ou d'exploitation inattendues ;

l) instructions de manipulation des supports (voir 7.10 et 7.14) ;

m) les procédures de redémarrage et de récupération du système à appliquer en cas de défaillance du système ;

n) la gestion du système de traçabilité et de l'information des journaux système (voir 8.15 et 8.17) et des systèmes de surveillance vidéo (voir 7.4) ;

o) les procédures de surveillance, notamment les capacités, les performances et la sécurité ;

p) les instructions de maintenance.

Il convient de passer en revue les procédures d'exploitation documentées et de les mettre à jour, si besoin. Il convient que les changements apportés aux procédures d'exploitation documentées soient approuvés par la direction. Lorsque cela est techniquement réalisable, il convient de gérer les systèmes d'information de façon homogène en utilisant des procédures, des outils et des utilitaires identiques.

Informations supplémentaires

Aucune autre information.

6 Mesures liées aux personnes

6.1 Présélection

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de réaliser des vérifications des références concernant tous les candidats à l'embauche avant qu'ils n'intègrent l'organisation puis de façon continue, conformément aux lois, aux réglementations et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

Objectif

S'assurer que tous les membres du personnel sont éligibles et compétents pour remplir les fonctions que l'organisation envisage de leur confier et qu'ils le restent tout au long de leur contrat de travail.

Préconisations

Il convient de réaliser un processus de présélection pour tout le personnel travaillant sous le contrôle de l'organisation, dont les salariés à plein temps et à temps partiel, les consultants et le personnel temporaire. Lorsque les contrats de ces personnes sont établis par l'intermédiaire de fournisseurs de services, il convient de préciser les exigences de présélection dans les accords contractuels entre l'organisation et les fournisseurs.

Il convient de rassembler et de traiter les informations sur tous les candidats envisagés pour des fonctions au sein de l'organisation conformément à toute législation appropriée en vigueur dans la juridiction concernée. En fonction de la législation applicable, il convient ou non d'informer au préalable les candidats de la procédure de sélection sur dossier.

Il convient que les vérifications prennent en compte le droit du travail et la législation relative à la protection de la vie privée et des données à caractère personnel, et que les vérifications comportent, dans les limites permises, les aspects suivants :

a) la production de références satisfaisantes, par exemple une référence professionnelle et une référence personnelle ;

b) une vérification (du degré d'exhaustivité et d'exactitude) du curriculum vitæ du candidat ;

c) la confirmation des formations et des qualifications professionnelles alléguées ;

d) un contrôle d'identité indépendant (passeport ou document similaire) ;

e) une vérification plus détaillée, par exemple un examen de la solvabilité ou du casier judiciaire si le candidat assume une fonction critique.

Lorsqu'une personne est embauchée pour assumer des fonctions spécifiques liées à la sécurité de l'information, il convient que l'organisation s'assure que le candidat :

a) possède les compétences nécessaires pour remplir ses fonctions ;

b) est digne de confiance, notamment si ses fonctions sont d'une grande importance pour l'organisation.

Qu'il s'agisse d'une première embauche ou d'une promotion, lorsqu'un poste implique l'accès aux moyens de traitement de l'information et, en particulier, s'il s'agit d'informations confidentielles, par exemple financières, à caractère personnel ou en rapport avec la santé, il convient que l'organisation envisage de procéder à des vérifications plus poussées et détaillées.

Il convient que les procédures définissent des critères et des limites à la réalisation des vérifications, par exemple qu'elles déterminent qui est habilité à contrôler les candidats, de quelle manière, à quel moment et pour quelles raisons.

Dans les cas où les vérifications ne peuvent pas être opérées dans les délais opportuns, il convient de mettre en œuvre des mesures d'atténuation et des contrôles d'accès réduits jusqu'à l'achèvement de la revue.

Il convient de réitérer les vérifications de façon régulière pour confirmer la compétence du personnel pour la fonction concernée, en fonction du niveau de criticité de cette dernière.

Informations supplémentaires

Aucune autre information.

6.2 Conditions générales d'embauche

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient que les contrats de travail précisent les responsabilités qui incombent au personnel et à l'organisation en matière de sécurité de l'information.

Objectif

S'assurer que le personnel comprend les responsabilités qui lui incombent quant à la sécurité de l'information dans le cadre de la fonction que l'organisation envisage de lui confier.

Préconisations

Il convient que les obligations contractuelles du personnel stipulent et précisent clairement les aspects suivants, en mettant en évidence la politique de sécurité de l'information et les politiques portant sur des thèmes de l'organisation :

a) il convient que le personnel ayant accès à des informations confidentielles signe un engagement de confidentialité ou de non-divulgation avant d'obtenir l'accès à l'information et aux autres actifs associés (voir 6.6) ;

b) les responsabilités juridiques et les droits du personnel concernant par exemple les droits d'auteur ou la législation sur la protection des données (voir 5.32 et 5.34) ;

c) les responsabilités relatives à la classification de l'information et à la gestion de l'information et des autres actifs associés de l'organisation, aux moyens de traitement de l'information et aux services d'information que le personnel utilise (voir 5.9 à 5.13) ;

d) les responsabilités du personnel en matière de traitement des informations reçues de la part des parties intéressées ;

e) les actions à engager si le personnel ne tient pas compte des exigences de sécurité de l'organisation (voir 6.4).

Lors du processus de préembauche, il convient d'informer clairement les candidats à l'embauche des rôles et des responsabilités en matière de sécurité.

Il convient que l'organisation s'assure que le personnel accepte les conditions générales relatives à la sécurité de l'information. Il convient que ces conditions générales soient en adéquation avec la nature et l'étendue de leur futur accès aux actifs de l'organisation liés aux services et aux systèmes d'information. Il convient de réviser les conditions générales relatives à la sécurité de l'information si les lois, les réglementations, la politique de sécurité de l'information ou les politiques portant sur des thèmes évoluent.

Si nécessaire, il convient que les responsabilités stipulées dans le contrat de travail continuent à s'appliquer pendant une durée définie après la fin du contrat (voir 6.5).

Informations supplémentaires

Il est possible de recourir à un code de conduite pour définir les responsabilités du personnel quant à la confidentialité, la protection des données à caractère personnel, l'éthique, l'utilisation appropriée de l'information et des autres actifs associés de l'organisation, ainsi qu'aux bonnes pratiques attendues par l'organisation en matière de sécurité de l'information.

Il peut s'avérer nécessaire d'intégrer une tierce partie, à laquelle le personnel du fournisseur est associé, aux accords contractuels passés au nom de la personne liée par le contrat.

Si l'organisation n'est pas une entité juridique et qu'elle n'emploie aucun salarié, l'équivalent de l'accord contractuel et des conditions générales peut être pris en compte conformément aux prescriptions de la présente mesure.

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

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient que le personnel de l'organisation et les parties intéressées soient sensibilisés et suivent un apprentissage et des formations à la sécurité de l'information adaptés, et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leur fonction.

Objectif

S'assurer que le personnel et les parties intéressées sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

Préconisations

Généralités

Il convient d'établir un programme de sensibilisation, d'apprentissage et de formation à la sécurité de l'information qui soit cohérent avec les politiques et procédures de l'organisation en matière de sécurité de l'information, et qui tienne compte des informations à protéger et des mesures mises en œuvre pour assurer cette protection.

Il convient que les sessions de sensibilisation, d'apprentissage et de formation à la sécurité de l'information aient lieu périodiquement. La sensibilisation initiale, l'apprentissage et la formation peuvent s'appliquer au nouveau personnel ou aux salariés mutés à de nouveaux postes ou assumant de nouvelles fonctions avec des exigences de sécurité de l'information nettement différentes.

Sensibilisation

Il convient que le programme de sensibilisation à la sécurité de l'information vise à sensibiliser le personnel aux responsabilités qui lui incombent en matière de sécurité de l'information et aux moyens dont il dispose pour s'acquitter de ces responsabilités.

Il convient de planifier le programme de sensibilisation en tenant compte des fonctions du personnel au sein de l'organisation, qu'il s'agisse du personnel interne ou externe (comme les consultants extérieurs ou le personnel des fournisseurs). Il convient que les activités prévues dans le programme de sensibilisation soient programmées dans le temps, de préférence à échéances régulières, de manière à se répéter et à inclure le nouveau personnel. Il convient également que le programme s'appuie sur les enseignements tirés des incidents liés à la sécurité de l'information.

Il convient que le programme de sensibilisation comporte un certain nombre d'activités permettant une meilleure sensibilisation via les canaux physiques ou virtuels appropriés, tels que des campagnes, livrets, posters, bulletins d'information, sites Web, sessions d'information, séances de briefing, modules d'e-apprentissage et e-mails. Il convient d'évaluer la compréhension par le personnel à l'issue de chaque activité de sensibilisation, d'apprentissage ou de formation afin de tester le transfert des connaissances et l'efficacité du programme de sensibilisation. Il convient que la sensibilisation à la sécurité de l'information couvre également des aspects généraux tels que :

a) la démonstration de l'engagement de la direction en faveur de la sécurité de l'information à tous les niveaux de l'organisation ;

b) la nécessité de se familiariser avec les règles et les obligations applicables à la sécurité de l'information, telles que définies dans la politique de sécurité de l'information et les politiques portant sur des thèmes, les normes, les lois, les statuts, les réglementations, les contrats et les accords, et de s'y conformer ;

c) l'imputabilité à chacun de ses actions et de son inaction, et les responsabilités générales en matière de sécurisation ou de protection des informations appartenant à l'organisation et aux parties intéressées ;

d) les procédures élémentaires en matière de sécurité de l'information (telles que le signalement des incidents liés à la sécurité de l'information) et les mesures de référence (telles que la sécurité des mots de passe, les mesures à l'encontre des programmes malveillants et la politique du bureau propre) ;

e) les points de contact et les ressources permettant d'obtenir des informations complémentaires et des conseils sur les questions de sécurité de l'information, y compris des documents complémentaires de sensibilisation.

Apprentissage et formation

Il convient que l'organisation identifie, élabore et mette en œuvre un plan de formation destiné aux équipes techniques dont les fonctions nécessitent un ensemble de compétences et une expertise spécifiques. Il convient que les équipes techniques disposent des compétences nécessaires pour configurer et gérer le niveau de sécurité requis des dispositifs, applications et services en nuage. Si des compétences s'avèrent manquantes, il convient que l'organisation prenne des mesures pour s'en doter.

Il convient de dispenser le programme d'apprentissage et de formation sous plusieurs formes, comme des présentations ou des autoformations, avec un encadrement par des experts ou des consultants (formation en milieu de travail), une rotation des membres du personnel pour suivre différentes activités, le recrutement de personnes déjà qualifiées et l'embauche de consultants. La formation peut être délivrée de différentes manières, par exemple en salle de cours, par apprentissage à distance, apprentissage en ligne, auto-apprentissage, etc. Il convient que le personnel technique maintienne ses connaissances à jour en s'abonnant à des bulletins d'information et des magazines ou en assistant à des conférences et à des événements destinés au perfectionnement technique et professionnel.

Il convient que les sessions d'apprentissage et de formation à la sécurité de l'information aient lieu périodiquement. Il convient d'appliquer l'apprentissage initial et la formation au nouveau personnel et aux salariés mutés à de nouveaux postes ou assumant de nouvelles fonctions avec des exigences de sécurité de l'information nettement différentes.

Informations supplémentaires

En élaborant un programme de sensibilisation, il est important de se concentrer sur les questions « quoi ? » et « comment ? », mais également sur la question « pourquoi ? ». Il est important que le personnel comprenne les enjeux de la sécurité de l'information et les conséquences éventuelles, positives et négatives, que leur comportement peut avoir sur l'organisation.

Sensibilisation, apprentissage et formation à la sécurité de l'information peuvent faire partie intégrante ou être associés à d'autres activités, par exemple une formation au management de l'information en général, aux TIC, à la sécurité ou à la protection des données personnelles.

6.4 Processus disciplinaire

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de formaliser et de communiquer un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et des autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information.

Objectif

S'assurer que le personnel et les autres parties intéressées comprennent les conséquences des violations de la sécurité de l'information et les dissuader d'effectuer des activités non conformes.

Préconisations

Il convient de ne pas déclencher le processus disciplinaire avant d'avoir vérifié l'existence d'un incident lié à la sécurité de l'information (voir 5.28).

Il convient que le processus disciplinaire formel prévoie une réponse graduée tenant compte des facteurs suivants :

a) la nature (qui, quoi, quand, comment) et la gravité de la violation et son impact sur l'activité ;

b) le caractère intentionnel (malveillant) ou non (accidentel) de l'infraction ;

c) le fait qu'il s'agisse d'une première infraction ou d'une récidive ;

d) si le contrevenant a reçu la formation adéquate.

Il convient que la réponse tienne compte des dispositions légales applicables, des contrats commerciaux et de tout autre facteur nécessaire. Il convient également que le processus disciplinaire constitue un élément dissuasif empêchant le personnel d'enfreindre la politique de sécurité de l'information, les politiques portant sur des thèmes et les procédures relatives à la sécurité de l'information. Les violations délibérées des règles peuvent nécessiter des mesures immédiates.

Informations supplémentaires

Il convient, dans la mesure du possible, de protéger l'identité des personnes faisant l'objet d'une mesure disciplinaire en cohérence avec la politique et les exigences de l'organisation.

Lorsqu'une personne a manifesté un très bon comportement à l'égard de la sécurité de l'information, une récompense peut lui être accordée afin de promouvoir la sécurité de l'information et le comportement de cette personne.

6.5 Responsabilités consécutivement à la fin ou à la modification du contrat de travail

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines #Gestion_des_actifs	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables consécutivement à la fin ou à la modification du contrat de travail, d'en informer le personnel concerné et les autres parties intéressées et de veiller à leur application.

Objectif

Protéger les intérêts de l'organisation dans le cadre du processus de modification ou de rupture d'une relation ou d'un contrat de travail.

Préconisations

Il convient que le processus de gestion de la fin ou de la modification du contrat de travail définisse les responsabilités et les missions liées à la sécurité de l'information qui restent valables consécutivement à la fin ou à la modification du contrat. Il peut s'agir de la confidentialité de l'information, de propriété intellectuelle et d'autres connaissances obtenues, ainsi que des responsabilités figurant dans tout autre engagement de confidentialité (voir 6.6). Il convient que les responsabilités et les missions encore valables après la fin de la relation ou du contrat de travail figurent dans les conditions générales d'embauche de la personne (voir 6.2), le contrat ou l'accord correspondant. Les autres contrats ou accords qui perdurent pendant une période définie après la fin du contrat de travail peuvent également contenir des responsabilités liées à la sécurité de l'information.

Il convient de gérer les changements de poste ou de responsabilités comme un terme mis au poste ou aux responsabilités en question, et de déterminer les nouvelles responsabilités ou les nouvelles fonctions.

Il convient d'identifier les fonctions et responsabilités liées à la sécurité de l'information assumées par la personne qui quitte son poste ou en change, et de les confier à une autre personne.

Il convient d'établir un processus pour communiquer les changements et les modalités de fonctionnement au personnel, aux autres parties intéressées et aux contacts pertinents (par exemple, clients et fournisseurs).

En outre, il convient d'appliquer le processus de gestion de la fin ou de la modification du contrat de travail au personnel externe (par exemple, les fournisseurs) en cas de rupture ou de fin du contrat ou du poste dans l'organisation, ou si un changement du poste intervient dans l'organisation.

Informations supplémentaires

Dans la plupart des organisations, le service des ressources humaines est généralement responsable de la totalité du processus de rupture ou de fin du contrat de travail et collabore avec le supérieur du salarié concerné pour gérer les aspects des procédures en lien avec la sécurité de l'information. Dans le cas du personnel mis à disposition par une tierce partie (par exemple, un fournisseur), le processus de fin d'emploi est géré par la tierce partie conformément aux termes du contrat conclu entre l'organisation et la tierce partie.

6.6 Engagements de confidentialité ou de non-divulgation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité	#Protection	#Sécurité_des_ressources_humaines #Protection_des_informations #Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème

Mesure de sécurité

Il convient d'identifier, de documenter, de revoir régulièrement et de signer des engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information.

Objectif

Gérer la confidentialité de l'information accessible au personnel ou à de tierces parties.

Préconisations

Il convient que les modalités des engagements de confidentialité ou de non-divulgation spécifient des exigences de protection de l'information confidentielle en des termes juridiquement exécutoires. Les engagements de confidentialité ou de non-divulgation sont applicables aux parties intéressées et au personnel de l'organisation. Selon les exigences de l'organisation en termes de sécurité de l'information, il convient de déterminer les termes des engagements en tenant compte du type d'information appelé à être traité, de son niveau de classification et de l'accès admissible par l'autre partie. Pour identifier les exigences en matière de confidentialité et de non-divulgation, il convient de tenir compte des éléments suivants :

a) une définition de l'information à protéger (par exemple, information confidentielle) ;

b) la durée prévue de l'engagement, y compris les cas où il peut s'avérer nécessaire de prolonger cette durée de façon illimitée ou jusqu'à ce que l'information tombe dans le domaine public ;

c) les actions à entreprendre lorsqu'un engagement arrive à expiration ;

d) les responsabilités et les tâches des signataires visant à éviter une divulgation non autorisée de l'information ;

e) la propriété de l'information, des secrets de fabrication et la propriété intellectuelle, ainsi que leurs liens avec la protection de l'information confidentielle ;

f) l'utilisation autorisée de l'information confidentielle et les droits du signataire relatifs à l'utilisation de ce type d'information ;

g) le droit d'auditer et de surveiller les activités impliquant l'utilisation de l'information confidentielle dans des circonstances hautement sensibles ;

h) le processus de notification et de signalement d'une divulgation non autorisée ou d'une fuite de l'information confidentielle ;

i) les modalités de restitution ou de destruction de l'information à l'expiration de l'accord ;

j) les actions à entreprendre en cas de violation de l'engagement.

Il convient que l'organisation prenne en compte la conformité des engagements de confidentialité et de non-divulgation pour la juridiction à laquelle ils s'appliquent (voir 5.31, 5.32, 5.33, 5.34).

Il convient de revoir les engagements de confidentialité et de non-divulgation à intervalles réguliers et en cas de changements ayant une incidence sur ces exigences.

Informations supplémentaires

Les engagements de confidentialité et de non-divulgation protègent l'information de l'organisation et informent les signataires de leur devoir de protéger, d'utiliser et de diffuser l'information de façon responsable et dans les limites autorisées.

En fonction des circonstances, une organisation peut devoir recourir à différentes formes d'engagements de confidentialité ou de non-divulgation.

6.7 Travail à distance

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Sécurité_système_et_réseau #Sécurité_physique	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient de mettre en œuvre des mesures de sécurité lorsque le personnel travaille à distance, pour protéger les informations consultées, traitées ou stockées en dehors des locaux de l'organisation.

Objectif

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

Préconisations

Le travail à distance consiste, pour le personnel de l'organisation, à travailler depuis un lieu situé en dehors des locaux de l'organisation, et à accéder à des informations imprimées sur papier ou enregistrées électroniquement via un équipement de TIC. Les environnements de travail à distance peuvent être désignés sous le nom de « télétravail », « travail à distance », « tiers lieu », « environnements de travail virtuels » et « maintenance à distance ».

Il convient que les organisations autorisant les activités de travail à distance se dotent d'une politique portant sur un thème qui définisse les conditions et les restrictions d'autorisation du travail à distance. Il convient d'envisager les aspects suivants si la loi l'autorise et que l'on estime qu'ils sont pertinents :

a) le niveau de sécurité physique en place ou proposé sur le site de travail à distance, en prenant en compte le niveau de sécurité physique du lieu et de l'environnement immédiat ;

b) les politiques portant sur le thème des mécanismes de sécurité pour l'environnement physique distant, tels qu'armoires de classement fermant à clé, transport sécurisé d'un lieu à l'autre et politiques portant sur le thème de l'accès distant, du bureau propre, de l'impression à distance et de l'élimination de l'information ;

c) les environnements de travail à distance physiques prévus ;

d) les exigences en matière de sécurité des communications, en tenant compte de la nécessité d'accéder à distance aux systèmes internes de l'organisation, de la sensibilité de l'information consultée ou transmise via le réseau de communication et de la sensibilité du système interne ;

e) l'utilisation de l'accès distant, tel que l'accès à un bureau virtuel, évitant le traitement et le stockage des informations sur un équipement détenu à titre privé ;

f) la menace que représente l'accès non autorisé aux informations ou ressources par d'autres personnes présentes sur le site de travail à distance, par exemple des membres de la famille et des amis ;

g) la menace que représente l'accès non autorisé aux informations ou aux ressources par d'autres personnes dans les lieux publics ;

h) l'utilisation de réseaux domestiques et de réseaux publics, et les exigences ou les restrictions relatives à la configuration des réseaux sans fil ;

i) les exigences relatives à la protection contre les programmes malveillants et au pare-feu ;

j) la vulnérabilité des mécanismes d'authentification à un seul facteur qui autorisent l'accès distant au réseau de l'organisation.

Il convient d'inclure aux lignes directrices et aux dispositions à prendre en compte :

a) la fourniture de l'équipement et des meubles de rangement adaptés aux activités de travail à distance, en cas d'interdiction d'utiliser un équipement détenu à titre privé et non soumis au contrôle de l'organisation ;

b) la définition des tâches autorisées, la classification des informations susceptibles d'être détenues, ainsi que les systèmes et services internes auxquels le travailleur à distance est autorisé à accéder ;

c) la mise en place d'une formation pour les personnes qui travaillent à distance et celles qui leur apportent de l'assistance. Il convient que cette formation explique comment réaliser son activité de manière sécurisée tout en travaillant à distance ;

d) la mise à disposition du matériel de communication adéquat, y compris les méthodes permettant de sécuriser l'accès distant, telles que les exigences relatives au verrouillage de l'écran de l'appareil et aux temporisateurs d'inactivité ; l'activation de la géolocalisation de l'appareil ; l'installation de fonctions d'effacement à distance ;

e) la sécurité physique ;

f) les règles et préconisations concernant l'accès de la famille et des visiteurs au matériel et aux informations ;

g) la fourniture de services d'assistance et de maintenance matérielles et logicielles ;

h) la souscription d'une assurance ;

i) les procédures relatives à la sauvegarde et à la continuité d'activité ;

j) l'audit et la surveillance liée à la sécurité ;

k) la révocation des droits d'utilisation et des droits d'accès, ainsi que la restitution du matériel au terme des activités de travail à distance.

Informations supplémentaires

Aucune autre information.

6.8 Signalement des événements liés à la sécurité de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient que l'organisation propose un mécanisme au personnel pour lui permettre de signaler dans les plus brefs délais les événements liés à la sécurité de l'information observés ou suspectés, par le biais des canaux appropriés.

Objectif

Permettre un signalement rapide, cohérent et efficace des événements liés à la sécurité de l'information qui peuvent être identifiés par le personnel.

Préconisations

Il convient d'informer tout le personnel et tous les utilisateurs de leur responsabilité de signaler le plus rapidement possible les événements liés à la sécurité de l'information de sorte à prévenir ou à réduire au minimum les conséquences des incidents liés à la sécurité de l'information. Il convient de les informer de l'existence d'une procédure de signalement des événements liés à la sécurité de l'information et d'un responsable servant de point de contact auprès duquel effectuer le signalement. Il convient que le mécanisme de signalement soit aussi simple, accessible et disponible que possible. Les événements liés à la sécurité de l'information recouvrent les incidents, les violations et les vulnérabilités.

Exemples de situations dans lesquelles envisager le signalement d'un événement :

a) une mesure de sécurité de l'information inefficace ;

b) une violation de la confidentialité de l'information, de son intégrité ou de sa disponibilité ;

c) une erreur humaine ;

d) la non-conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes ou aux normes ;

e) une violation des dispositions relatives à la sécurité physique ;

f) un changement non contrôlé apporté au système ;

g) un dysfonctionnement ou autre comportement anormal du système au niveau logiciel ou matériel ;

h) une violation d'accès ;

i) des vulnérabilités ;

j) la suspicion d'une infection par un logiciel malveillant.

Il convient de recommander au personnel et aux utilisateurs de ne pas tenter de démontrer l'existence des failles de sécurité de l'information suspectées. Rechercher les failles pourrait être interprété comme un mauvais usage potentiel du système. La recherche peut en outre endommager le système d'information ou le service et risquer d'altérer ou de masquer une preuve numérique. Enfin, elle peut exposer la personne la réalisant à des poursuites judiciaires.

Informations supplémentaires

Pour de plus amples informations, voir l'ISO/IEC 27035 (toutes les parties).

7 Contrôles physiques

7.1 Périmètre de sécurité physique

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de définir des périmètres de sécurité servant à protéger les zones qui contiennent l'information sensible ou critique et les autres actifs associés.

Objectif

Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les autres actifs associés de l'organisation.

Préconisations

Le cas échéant, il convient d'envisager et de mettre en œuvre les lignes directrices suivantes concernant les périmètres de sécurité physique :

a) il convient de définir des périmètres de sécurité et il convient que l'emplacement et le niveau de résistance de chacun des périmètres soient fonction des exigences relatives à la sécurité des actifs situés à l'intérieur et des conclusions de l'appréciation du risque ;

b) il convient que le périmètre d'un bâtiment ou d'un site abritant des moyens de traitement de l'information soit physiquement solide (il convient que le périmètre ou les zones ne présentent aucune faille susceptible de faciliter une intrusion). Il convient que le toit, les murs extérieurs, les plafonds et le sol du site soient construits de manière solide et que les portes extérieures soient toutes convenablement protégées contre les accès non autorisés par des mécanismes de contrôle (par exemple, barres, alarmes, verrous). Il convient également de verrouiller les portes et les fenêtres non gardées, et d'envisager une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée, et de prévoir des aérations ;

c) il convient de mettre en place une zone de réception surveillée par du personnel, ou d'autres moyens permettant de contrôler l'accès physique au site ou au bâtiment ;

d) il convient d'équiper d'une alarme l'ensemble des portes coupe-feu du périmètre de sécurité, de surveiller ces portes et de les tester en même temps que les murs, pour établir le niveau de résistance requis conformément aux normes appropriées. Il convient qu'elles fonctionnent conformément au code local de prévention des incendies et de manière infaillible ;

e) il convient d'installer des systèmes de détection d'intrusion adaptés, conformes aux normes nationales, régionales et internationales, et de les tester régulièrement pour s'assurer qu'ils englobent l'ensemble des portes extérieures et des fenêtres accessibles. Il convient que les alarmes des zones inoccupées soient activées en permanence. Il convient également de couvrir les autres zones, comme la salle informatique ou la salle des télécommunications.

Informations supplémentaires

La protection physique peut être assurée en créant une ou plusieurs barrières physiques autour des locaux et des moyens de traitement de l'information de l'organisation. L'utilisation de barrières multiples offrant un surcroît de protection, la défaillance d'une seule barrière ne compromet pas directement la sécurité.

La zone sécurisée peut être un bureau fermé à clé ou un ensemble de plusieurs salles ceint d'une barrière de sécurité physique interne continue. Des barrières et des périmètres supplémentaires de contrôle d'accès physique peuvent s'avérer nécessaires entre des zones soumises à des exigences de sécurité différentes à l'intérieur d'un même périmètre de sécurité. Il convient que l'organisation envisage la mise en place de mesures de sécurité physique pouvant être renforcées au cours des situations d'intensification des menaces.

7.2 Contrôles physiques des accès

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Intégrité #Disponibilité #Confidentialité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de protéger les zones sécurisées par des contrôles d'accès et des points d'accès appropriés.

Objectif

Garantir l'accès physique à l'information et aux autres actifs associés de l'organisation par le biais d'autorisations seulement.

Préconisations

Généralités

Il convient de surveiller les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux et, si possible, de les isoler des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

Il convient de tenir compte des lignes directrices suivantes :

a) il convient de limiter l'accès aux sites et aux bâtiments au seul personnel autorisé. Il convient que le processus de gestion des droits d'accès aux zones physiques comprenne la fourniture, la revue périodique, la mise à jour et la révocation des autorisations (voir 5.18) ;

b) il convient de conserver de manière sécurisée et de contrôler régulièrement un journal physique ou un système de traçabilité électronique de tous les accès, et de protéger l'ensemble des journaux et des informations d'authentification sensibles (voir 5.33) ;

c) il convient d'établir et de mettre en œuvre un processus et des mécanismes techniques pour la gestion de l'accès aux zones de traitement ou de stockage de l'information. Les systèmes d'authentification incluent l'utilisation de cartes d'accès, la biométrie ou l'authentification à deux facteurs, tels qu'une carte d'accès et un code PIN secret. Il convient d'envisager l'installation de sas de sécurité pour l'accès aux zones sensibles ;

d) il convient d'inspecter et d'examiner les effets personnels des salariés à l'entrée et à la sortie ;

e) il convient d'exiger de l'ensemble du personnel et des parties intéressées le port d'un moyen d'identification visible. Il convient qu'ils informent immédiatement le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d'identification visible. Il convient d'envisager le port de badges faciles à distinguer pour mieux identifier les salariés permanents, les fournisseurs et les visiteurs ;

f) il convient d'accorder au personnel des fournisseurs un accès limité aux zones sécurisées ou aux moyens de traitement de l'information et uniquement en fonction des nécessités. Il convient que cet accès fasse l'objet d'une autorisation et d'une surveillance ;

g) il convient de porter une attention spéciale à la sécurité des accès physiques dans le cas de bâtiments renfermant les actifs de plusieurs organisations ;

h) il convient de mettre en place des mesures de sécurité physique pouvant être renforcées au cours des situations d'intensification des menaces ;

i) il convient de protéger les autres points d'accès, tels que les sorties de secours, de tout accès non autorisé ;

j) il convient de mettre en place des procédures de gestion garantissant que seules les personnes autorisées ont accès aux clés physiques ou aux informations d'authentification telles que les codes de verrouillage (voir 5.17 pour des recommandations supplémentaires).

Visiteurs

Il convient de tenir compte des lignes directrices suivantes :

a) il convient d'authentifier l'identité des visiteurs à l'aide d'un moyen approprié ;

b) il convient de consigner la date et l'heure d'arrivée et de départ des visiteurs ;

c) il convient d'accorder l'accès aux visiteurs uniquement à des fins précises ayant fait l'objet d'une autorisation et de leur remettre les instructions relatives aux exigences de sécurité de la zone et aux procédures d'urgence associées ;

d) il convient d'encadrer tous les visiteurs, sauf si une exception explicite leur a été accordée.

Zones de livraison et de chargement et réception de matériel

Il convient de tenir compte des lignes directrices suivantes :

a) il convient que l'accès aux zones de livraison et de chargement depuis l'extérieur du bâtiment soit limité au personnel identifié et autorisé ;

b) il convient de concevoir les zones de livraison et de chargement de sorte que les livraisons puissent être chargées et déchargées sans que le personnel n'ait accès sans y être autorisé aux autres parties du bâtiment ;

c) il convient de sécuriser les portes extérieures des zones de livraison et de chargement lorsque les portes menant aux zones restreintes sont ouvertes ;

d) il convient d'inspecter les réceptions pour vérifier la présence éventuelle de substances explosives, chimiques ou autres substances dangereuses, avant qu'elles ne quittent les zones de livraison et de chargement ;

e) il convient d'enregistrer les réceptions conformément aux procédures de gestion des actifs (voir 5.9 et 7.10) dès leur arrivée sur le site ;

f) dans la mesure du possible, il convient de séparer physiquement les livraisons des expéditions ;

g) il convient d'inspecter les réceptions pour vérifier la présence d'éventuelles altérations survenues lors de l'acheminement. Il convient de prévenir immédiatement le personnel de sécurité de toute découverte de ce type.

Informations supplémentaires

Aucune autre information.

7.3 Sécurisation des bureaux, des salles et des équipements

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient de concevoir et de mettre en œuvre des mesures de sécurité physique pour les bureaux, les salles et les équipements.

Objectif

Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les autres actifs associés de l'organisation dans les bureaux, salles et équipements.

Préconisations

Il convient de prendre en compte les lignes directrices suivantes sur la sécurisation des bureaux, des salles et des équipements :

a) pour les équipements-clés, il convient de choisir un emplacement non accessible au public ;

b) dans la mesure du possible, il convient que les bâtiments soient discrets et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur, qui permette d'identifier la présence d'activités de traitement de l'information ;

c) il convient que les équipements soient configurés de manière à empêcher que l'information confidentielle ou les activités soient visibles et audibles de l'extérieur. Si nécessaire, il convient d'envisager la mise en place d'un bouclier électromagnétique ;

d) il convient que les répertoires et annuaires téléphoniques internes, ainsi que les cartes accessibles en ligne identifiant l'emplacement des moyens de traitement de l'information confidentielle ne soient pas accessibles sans autorisation ;

e) il convient que l'organisation mette en place une procédure permettant de gérer les clés physiques ou les serrures à combinaison des bureaux, salles et équipements, tels qu'une armoire fermant à clé, un journal ou un contrôle annuel des clés.

Informations supplémentaires

Aucune autre information.

7.4 Surveillance de la sécurité physique

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Sécurité_physique	#Protection #Défense

Mesure de sécurité

Il convient que les locaux fassent l'objet d'une surveillance continue concernant l'accès physique non autorisé.

Objectif

Détecter et empêcher tout accès physique non autorisé.

Préconisations

Il convient de contrôler les locaux physiques à l'aide de systèmes de surveillance, qu'il s'agisse de vigiles, d'alarmes anti-intrusion ou de systèmes de vidéosurveillance tels que des télévisions en circuit fermé et un logiciel de gestion de l'information de sécurité physique géré en interne ou par un prestataire de services de surveillance.

Il convient que l'accès aux bâtiments qui hébergent des systèmes critiques fasse l'objet d'une surveillance continue pour détecter tout accès non autorisé ou comportement suspect :

a) installation de systèmes de vidéosurveillance tels que des télévisions en circuit fermé permettant de visionner et d'enregistrer l'accès aux zones sensibles à l'intérieur et à l'extérieur des locaux de l'organisation ;

b) installation et test régulier de détecteurs de contact, de son ou de mouvement qui déclenchent une alarme anti-intrusion :

   1) les détecteurs de contact déclenchent une alarme lorsqu'un contact est coupé ; il convient de les installer à tout endroit où un contact peut être établi ou coupé, tel que les fenêtres, les portes et sous les objets, en vue de servir d'alarme d'urgence ;

   2) les détecteurs de mouvements, basés sur la technologie infrarouge, déclenchent une alarme lorsqu'un objet passe dans leur champ de vision ;

   3) l'installation de capteurs sensibles au son du bris de verre permet de déclencher une alarme pour alerter le personnel de sécurité.

Il convient de garder la conception des systèmes de surveillance confidentielle, car une divulgation peut faciliter des intrusions non détectées.

Il convient de placer le tableau de commande du système d'alarme dans une zone équipée d'une alarme et, dans le cas des alarmes de sécurité, dans un endroit offrant une sortie facile d'accès pour la personne qui active l'alarme. Il convient que le tableau de commande et les détecteurs soient équipés de systèmes inviolables. Il convient de tester régulièrement le système pour s'assurer qu'il fonctionne conformément aux attentes, en particulier si ses composants sont alimentés par batterie.

Il convient d'utiliser tout système de surveillance et d'enregistrement conformément aux lois et réglementations locales, y compris législation relative à la protection des données et des DCP, notamment en ce qui concerne la surveillance des travailleurs et la durée de conservation des vidéos.

Informations supplémentaires

Aucune autre information.

7.5 Protection contre les menaces physiques et environnementales

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de concevoir et de mettre en œuvre une protection contre les menaces physiques et environnementales telles que les catastrophes naturelles et autres menaces physiques volontaires ou non liées à l'infrastructure.

Objectif

Prévenir les événements ayant pour origine des menaces physiques ou environnementales ou réduire leur impact.

Préconisations

Il convient de réaliser des appréciations des risques concernant l'impact potentiel des menaces physiques et environnementales avant de lancer des opérations critiques sur un site physique, ce à intervalles réguliers. Il convient de mettre en œuvre les protections nécessaires et de surveiller les changements des menaces. Il convient de solliciter les conseils de spécialistes sur la gestion des risques liés aux menaces physiques et environnementales, telles que les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou d'origine humaine.

Il convient que l'emplacement et la construction des locaux tiennent compte des éléments suivants :

a) topographie locale, telle que l'élévation appropriée, les cours d'eau et les failles tectoniques ;

b) les menaces urbaines, telles que les lieux ayant une forte probabilité d'attirer de l'agitation politique, des activités criminelles ou des attaques terroristes.

En fonction des résultats des appréciations des risques, il convient d'identifier les menaces physiques et environnementales pertinentes et d'envisager les mesures de sécurité appropriées dans les contextes suivants, par exemple :

a) Incendie : il convient d'installer des systèmes capables de détecter les incendies à leur tout début et de les configurer en vue du déclenchement d'alarmes ou de systèmes d'extinction d'incendie afin de prévenir les dommages du feu sur les supports de stockage de l'information et sur les systèmes de traitement de l'information associés. Il convient de procéder à l'extinction d'incendie avec la substance la plus efficace par rapport au milieu ambiant (par exemple, le gaz dans les centres de données) ;

b) Inondation : il convient d'installer des systèmes capables de détecter les inondations à leur tout début, sous le sol des zones contenant des supports de stockage de l'information ou d'en équiper les systèmes de traitement de l'information associés. Il convient de prévoir des pompes à eau ou des moyens équivalents prêts à l'emploi en cas de survenue d'une inondation ;

c) Surtension : il convient d'adopter des systèmes capables de protéger les systèmes d'information client aussi bien que serveur contre les surtensions ou événements similaires afin de réduire au minimum les conséquences de tels événements ;

d) Explosifs et armes : il convient de procéder à des inspections aléatoires pour s'assurer de l'absence d'explosifs ou d'armes sur le personnel, dans les véhicules ou dans les marchandises pénétrant dans des moyens de traitement de l'information sensible.

Informations supplémentaires

Les organisations peuvent examiner les concepts de prévention de la criminalité par la conception environnementale (ou CPTED pour Crime Prevention Through Environmental Design) pour concevoir les mesures destinées à protéger leur environnement et à réduire les menaces urbaines. Par exemple, au lieu d'utiliser des bornes, la mise en œuvre de statues ou de pièces d'eau peut servir à la fois d'aménagement et de barrière physique.

7.6 Travail dans les zones sécurisées

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de concevoir et de mettre en œuvre des procédures pour le travail en zone sécurisée.

Objectif

Empêcher tout dommage ou intrusion portant sur l'information et les autres actifs associés de l'organisation dans les zones sécurisées.

Préconisations

Il convient que les dispositions et mesures relatives au travail en zone sécurisée s'appliquent à tout le personnel et qu'elles concernent toutes les activités se déroulant dans ces zones.

Il convient de tenir compte des lignes directrices suivantes :

a) il convient que le personnel soit informé de l'existence de zones sécurisées ou des activités qui s'y pratiquent, sur la seule base du besoin d'en connaître ;

b) il convient d'éviter le travail non supervisé/encadré en zone sécurisée, tant pour des raisons de sécurité personnelle que pour prévenir tout acte malveillant ;

c) il convient de verrouiller physiquement et de contrôler périodiquement les zones sécurisées inoccupées ;

d) il convient d'interdire tout matériel photographique, vidéo, audio ou autre matériel d'enregistrement, tel que les appareils photos intégrés aux terminaux utilisateurs, sauf autorisation ;

e) il convient d'appliquer les contrôles appropriés au port et à l'utilisation de terminaux utilisateurs finaux dans les zones sécurisées ;

f) il convient de publier des procédures d'urgence facilement visibles ou accessibles.

Informations supplémentaires

Aucune autre information.

7.7 Bureau propre et écran vide

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de définir et d'appliquer les règles du bureau propre pour les documents papier et les supports de stockage amovibles, et les règles de l'écran vide pour les moyens de traitement de l'information.

Objectif

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

Préconisations

Il convient que l'organisation établisse et communique à toutes les parties intéressées une politique portant sur le thème du bureau propre et de l'écran vide.

Il convient de tenir compte des lignes directrices suivantes :

a) lorsque l'information sensible ou critique liée à l'activité de l'organisation n'est pas utilisée, qu'elle soit sous format papier ou sur un support de stockage électronique, il convient de la mettre sous clé (de préférence dans un coffre-fort, une armoire ou tout autre meuble de sécurité), notamment lorsque les locaux sont vides ;

b) il convient de protéger les terminaux utilisateurs par des serrures à clé ou tout autre moyen de sécurité physique lorsqu'ils ne sont pas utilisés ou sont laissés sans surveillance ;

c) lorsque les ordinateurs et les terminaux sont laissés sans surveillance, il convient de les déconnecter ou de les protéger par un verrouillage de l'écran ou du clavier contrôlé par un mot de passe, un jeton ou un autre mécanisme d'authentification de l'utilisateur. Il convient de configurer tous les ordinateurs et systèmes avec un délai d'attente ou une fonction de fermeture de session automatique ;

d) il convient de stocker de façon sécurisée les documents contenant de l'information sensible en provenance de dispositifs multifonctions, tels que des imprimantes et autres technologies de reproduction et, lorsqu'ils ne sont plus utilisés, de les mettre au rebut à l'aide de mécanismes d'élimination sécurisés ;

e) il convient d'établir et de communiquer des règles et recommandations relatives à la configuration des fenêtres contextuelles affichées à l'écran (par exemple, il convient de désactiver les fenêtres contextuelles de réception de courrier électronique et de messages instantanés, si possible, durant les présentations, en cas de partage d'écran ou dans les lieux publics) ;

f) il convient d'effacer les tableaux blancs et autres types d'affichage lorsqu'ils ne sont plus nécessaires.

Il convient que l'organisation mette en place des procédures applicables au moment de quitter les locaux, notamment la réalisation d'un dernier passage avant de partir pour s'assurer de ne laisser aucun actif de l'organisation, par exemple des documents tombés derrière un tiroir ou un meuble.

Informations supplémentaires

L'utilisation de coffres forts ou d'autres moyens de stockage sécurisés peut également contribuer à la protection de l'information contre les sinistres tels qu'incendies, tremblements de terre, inondations ou explosions.

Envisager l'utilisation d'imprimantes dotées d'une fonction d'identification par code personnel, afin que seules les personnes ayant lancé l'impression puissent récupérer les documents imprimés et uniquement lorsqu'elles se trouvent à proximité de l'imprimante.

7.8 Emplacement et protection du matériel

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient de disposer le matériel de façon sécurisée et de le protéger.

Objectif

Réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé.

Préconisations

Il convient de prendre en compte les lignes directrices suivantes pour protéger le matériel :

a) il convient de déterminer un emplacement pour le matériel permettant de réduire au minimum les accès inutiles aux zones de travail ;

b) il convient de positionner avec soin les moyens de traitement de l'information manipulant des données sensibles, en vue de réduire le risque que cette information puisse être vue par des personnes non autorisées ;

c) il convient de sécuriser les moyens de stockage contre tout accès non autorisé ;

d) il convient d'adopter des mesures visant à réduire au minimum les risques de menaces physiques et environnementales potentielles, comme le vol, l'incendie, les explosions, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau), la poussière, les vibrations, les effets engendrés par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme ;

e) il convient de fixer des lignes directrices sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information ;

f) il convient de surveiller les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information ;

g) il convient d'équiper l'ensemble des bâtiments d'un paratonnerre et il convient d'équiper toutes les lignes électriques et de télécommunication entrantes de parafoudres ;

h) il convient d'envisager l'utilisation de méthodes spéciales de protection, telles que les claviers à membrane, pour le matériel utilisé en environnement industriel ;

i) il convient de protéger les moyens de traitement de l'information confidentielle pour réduire au minimum les risques de fuites d'information dues aux émissions électromagnétiques ;

j) il convient de séparer physiquement les moyens de traitement de l'information gérés par l'organisation de ceux qu'elle ne gère pas.

Informations supplémentaires

Aucune autre information.

7.9 Sécurité des actifs hors des locaux

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient de protéger les actifs hors du site en prenant en compte les différents risques.

Objectif

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

Préconisations

Tout dispositif utilisé en dehors des locaux de l'organisation pour stocker ou traiter de l'information (par exemple, appareil mobile), qu'il s'agisse de dispositifs détenus par l'organisation ou de dispositifs détenus à titre privé et utilisés pour le compte de l'organisation (AVEC), doit être protégé. Il convient que l'utilisation des dispositifs de ce type soit autorisée par l'organisation.

Il convient de tenir compte des lignes directrices suivantes concernant la protection du matériel destiné à stocker ou à traiter l'information en dehors des locaux de l'organisation :

a) il convient de ne pas laisser le matériel et les supports de données sortis des locaux sans surveillance dans les lieux publics et non sécurisés ;

b) il convient d'observer à tout instant les instructions du fabricant visant à protéger le matériel, par exemple celles sur la protection contre les champs électromagnétiques forts, l'eau, la chaleur, l'humidité et la poussière ;

c) lorsque du matériel circule hors des locaux de l'organisation entre différentes personnes ou entre des parties intéressées, il convient de tenir à jour un journal détaillant la chaîne de traçabilité du matériel et indiquant au minimum les noms des personnes responsables du matériel, ainsi que les organisations dont elles relèvent. Avant le transfert, il convient de supprimer de façon sécurisée toute information qu'il n'est pas nécessaire de communiquer en même temps que l'actif ;

d) si nécessaire et réalisable, il convient d'exiger une autorisation pour le retrait de matériel et d'information des locaux de l'organisation et de garder un enregistrement des retraits correspondants pour en assurer la traçabilité ;

e) protection contre la consultation d'information sur un dispositif, tel qu'un appareil mobile ou un ordinateur portable dans les transports publics, et les risques associés au fait de « regarder par-dessus l'épaule ».

Le matériel tel que les antennes et les GAB situés hors des locaux de l'organisation peut être soumis à un risque plus élevé de dommage, de vol ou d'interception, et peut différer de façon considérable d'un lieu à l'autre ; il convient de le prendre en compte pour déterminer les mesures les mieux appropriées. Il convient de tenir compte des lignes directrices suivantes pour déterminer où installer ce matériel hors des locaux de l'organisation :

a) surveillance de la sécurité physique (voir 7.4) ;

b) protection contre les menaces physiques et environnementales (voir 7.5) ;

c) mesures liées à l'accès physique et à l'inviolabilité ;

d) contrôles d'accès logique.

Informations supplémentaires

De plus amples informations sur les autres aspects de la protection du matériel servant à stocker et traiter de l'information et des terminaux utilisateurs sont disponibles en 8.1 et 6.7.

Il peut être pertinent, pour éviter tout risque, de dissuader certains salariés de travailler en dehors des locaux de l'organisation ou de restreindre l'utilisation de leur équipement de TIC portable.

7.10 Supports de stockage

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient de gérer les supports de stockage tout au long de leur cycle de vie d'acquisition, d'utilisation, de transport et de mise au rebut conformément au plan de classification et aux exigences de manipulation de l'organisation.

Objectif

S'assurer de la divulgation, de la modification, du retrait ou de la destruction de l'information de l'organisation stockée sur des supports par le biais d'autorisations seulement.

Préconisations

Supports amovibles

Il convient de tenir compte des lignes directrices suivantes concernant la gestion des supports amovibles :

a) il convient que l'organisation établisse une politique portant sur le thème de la gestion des supports amovibles et qu'elle communique ladite politique portant sur un thème à toute personne qui utilise ou manipule des supports amovibles ;

b) si nécessaire et réalisable, il convient d'exiger une autorisation pour le retrait de supports de l'organisation et de garder un enregistrement de ces retraits pour en assurer la traçabilité ;

c) il convient de stocker tous les supports dans un environnement sûr, sécurisé et conforme à la classification de l'information correspondante, et de les protéger des menaces environnementales (telles que l'exposition à la chaleur, à une humidité plus ou moins forte, aux champs électromagnétiques ou le vieillissement) conformément aux spécifications du fabricant ;

d) si la confidentialité ou l'intégrité de l'information constitue un facteur important, il convient d'utiliser des techniques cryptographiques pour protéger l'information stockée sur support amovible ;

e) pour atténuer les risques liés à la dégradation du support lorsque l'information stockée est encore nécessaire, il convient de transférer cette information sur un support neuf, avant qu'elle ne devienne illisible ;

f) il convient de stocker plusieurs copies de l'information de valeur sur des supports séparés pour réduire les risques concomitants d'endommagement ou de perte de l'information ;

g) il convient d'envisager de tenir un registre des supports amovibles pour limiter les risques de perte d'information ;

h) il convient de n'autoriser les ports de supports amovibles, comme les emplacements pour carte SD ou les ports USB, que si l'organisation a une raison de les utiliser ;

i) lorsqu'il est nécessaire d'utiliser des supports amovibles, il convient de contrôler le transfert de l'information sur ces supports.

Transport sécurisé

Il convient de prendre en compte les lignes directrices suivantes pour protéger les supports d'information lors de leur transport :

a) il convient que le transporteur ou le coursier employé soit fiable ;

b) il convient d'établir, en accord avec la direction, la liste des coursiers autorisés ;

c) il convient de mettre au point des procédures de contrôle de l'identification des coursiers ;

d) il convient que l'emballage choisi soit suffisant pour protéger son contenu de tout dommage physique susceptible de survenir lors du transit et qu'il soit conforme aux spécifications du fabricant en fournissant par exemple une protection contre tout facteur environnemental pouvant diminuer l'efficacité de la restauration du support, comme l'exposition à de fortes températures, à une forte humidité ou à des champs électromagnétiques ;

e) selon le niveau de classification de l'information ou du support à transporter, il convient de recourir à des mesures anti-effraction comme des pochettes, des sacoches ou des conteneurs ;

f) il convient de conserver les journaux identifiant le contenu du support, la protection appliquée, ainsi que la liste des destinataires autorisés, les dates et heures de remise aux responsables du transport et de réception par le destinataire.

Réutilisation ou élimination sécurisée

Il convient que les procédures de réutilisation ou d'élimination sécurisée des supports réduisent au minimum le risque de fuite d'information confidentielle vers des personnes non autorisées. Il convient que les procédures de réutilisation ou d'élimination sécurisée des supports contenant de l'information confidentielle soient proportionnelles à la sensibilité de cette information. Il convient d'envisager les éléments suivants :

a) dans le cas d'un support contenant de l'information confidentielle, il convient de supprimer les données ou de les formater avant de les réutiliser (voir 8.10) ;

b) il convient d'éliminer les supports contenant de l'information confidentielle de façon sécurisée, par exemple par incinération ou déchiquetage ;

c) il convient de mettre en place des procédures d'identification des éléments pouvant nécessiter une élimination sécurisée ;

d) de nombreuses organisations proposent des services de collecte et d'enlèvement des supports ; il convient de sélectionner avec soin le fournisseur tiers approprié disposant de mesures de sécurité et d'une expérience suffisantes ;

e) il convient de journaliser l'élimination des éléments sensibles pour en assurer la traçabilité ;

f) en cas d'accumulation de supports en vue de leur élimination, il convient de prendre en compte l'effet d'agrégation qui peut rendre sensible une grande quantité d'information à l'origine non confidentielle.

Informations supplémentaires

Les appareils endommagés contenant des données sensibles peuvent nécessiter une appréciation du risque visant à déterminer s'il convient de les détruire physiquement plutôt que de les envoyer en réparation ou de les mettre au rebut (voir 7.14).

L'information peut être vulnérable à un accès non autorisé, à une utilisation frauduleuse ou à une altération pendant le transport physique, par exemple lors de l'envoi de supports par courrier ou par coursier. Cette mesure concerne également les documents papier.

Lorsque les supports contiennent une information confidentielle non cryptée, il convient d'envisager une protection physique supplémentaire.

Des mesures visant à empêcher ou limiter l'utilisation de supports amovibles peuvent compléter ou rendre inutiles les dispositions décrites dans cette mesure de sécurité.

7.11 Services généraux

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Disponibilité	#Protection #Détection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de protéger les moyens de traitement de l'information des coupures de courant et autres perturbations dues à une défaillance des services collectifs.

Objectif

Empêcher la perte, l'endommagement ou la compromission de l'information et des autres actifs associés en raison de la défaillance et de la perturbation des services collectifs ou de l'interruption des activités de l'organisation.

Préconisations

Les organisations sont tributaires de services collectifs (tels que l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation et la climatisation) pour le soutien de leurs moyens de traitement de l'information. Par conséquent, il convient que le matériel de l'organisation qui permet l'accès aux services collectifs et la fourniture de ces derniers :

a) soit conforme aux spécifications du fabricant du matériel et aux exigences légales, statutaires ou réglementaires locales ;

b) fasse l'objet d'une évaluation régulière pour vérifier sa capacité à répondre à la croissance de l'organisation et aux interactions avec les autres services généraux ;

c) soit examiné et testé de manière régulière pour s'assurer de son bon fonctionnement ;

d) soit équipé, si nécessaire, d'alarmes de détection des dysfonctionnements ;

e) dispose, si nécessaire, d'alimentations multiples sur les réseaux physiques d'acheminement ;

f) lorsqu'il est connecté à un réseau, se trouve sur un autre réseau que les moyens de traitement de l'information ;

g) soit connecté à Internet uniquement en cas de nécessité et de façon sécurisée ;

h) garantisse la consignation des coordonnées des personnes à contacter en cas d'urgence et leur mise à disposition au personnel en cas de panne.

Il convient que soient prévus des systèmes d'éclairage et de communication d'urgence. Il convient de placer les interrupteurs et les robinets de secours destinés à couper le courant, l'eau, le gaz ou autres services près des sorties de secours et/ou des salles contenant le matériel.

Informations supplémentaires

Il est possible de disposer de connexions réseau supplémentaires en faisant appel à plusieurs fournisseurs de service.

7.12 Sécurité du câblage

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Disponibilité	#Protection	#Sécurité_physique	#Protection

Mesure de sécurité

Il convient de protéger les câbles électriques, transportant des données ou supportant les services d'information contre toute interception, interférence ou tout dommage.

Objectif

Empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation en raison de la défaillance des câbles électriques et de télécommunications.

Préconisations

Il convient de prendre en compte les lignes directrices suivantes sur la sécurité du câblage :

a) enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou les soumettre à toute autre forme de protection adéquate, telle qu'un dispositif de protection des câbles au sol et un poteau électrique ; si les câbles sont enterrés, les protéger de toute coupure accidentelle, par exemple par un blindage ou des signaux de présence ;

b) séparer les câbles électriques des câbles de télécommunications pour éviter toute interférence ;

c) pour les systèmes sensibles ou critiques, les mesures supplémentaires à envisager comprennent :

   1) l'installation d'un conduit de câbles blindés et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités ;

   2) l'utilisation d'un blindage électromagnétique pour assurer la protection des câbles ;

   3) le déclenchement de balayages techniques et d'inspections physiques pour détecter le branchement d'appareils non autorisés sur les câbles ;

   4) un accès contrôlé aux panneaux de répartition et aux chambres de câblage (par exemple, avec des clés mécaniques ou des codes PIN) ;

   5) l'utilisation de câbles à fibre optique ;

d) l'étiquetage des câbles à chaque extrémité avec suffisamment de détails sur la source et la destination pour permettre l'identification physique et l'inspection du câble.

Dans certains cas, les câbles électriques et de télécommunications sont des ressources partagées par plusieurs organisations occupant des locaux communs.

Informations supplémentaires

Aucune autre information.

7.13 Maintenance du matériel

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection #Résilience

Mesure de sécurité

Il convient d'entretenir le matériel correctement.

Objectif

Empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation.

Préconisations

Il convient de prendre en compte les lignes directrices suivantes sur la maintenance du matériel :

a) entretenir le matériel selon les spécifications et la périodicité recommandées par le fournisseur ;

b) mettre en œuvre un programme d'entretien et assurer son suivi par l'organisation ;

c) faire effectuer les réparations et l'entretien du matériel par le seul personnel de maintenance autorisé ;

d) consigner toutes les pannes suspectées ou avérées et toutes les tâches de maintenance préventive ou corrective ;

e) mettre en œuvre des mesures appropriées lorsque la maintenance d'un matériel est programmée, en prenant en compte le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'organisation ; soumettre le personnel de maintenance à un engagement de confidentialité approprié ;

f) superviser le personnel de maintenance lors de la réalisation de la maintenance sur site ;

g) autoriser la maintenance du matériel à distance et mettre en œuvre des mesures visant à empêcher tout accès non autorisé ;

h) appliquer la mesure de sécurité 7.9 si du matériel contenant de l'information est sorti des locaux à des fins de maintenance ;

i) se conformer à toutes les exigences de maintenance imposées par l'assurance ;

j) avant de remettre le matériel en service à l'issue de sa maintenance, l'inspecter pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement ;

k) appliquer la mesure de sécurité 7.14 s'il s'avère que le matériel doit être mis au rebut.

Informations supplémentaires

Le matériel comprend les dispositifs d'alimentation continue et les batteries, les groupes électrogènes, les alternateurs et les commutateurs, les systèmes de détection des intrusions physiques et les alarmes, les détecteurs de fumée, les extincteurs et les ascenseurs.

7.14 Mise au rebut ou recyclage sécurisé(e) du matériel

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection

Mesure de sécurité

Il convient de vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.

Objectif

Éviter la fuite d'information du matériel à réutiliser ou à mettre au rebut.

Préconisations

Avant la mise au rebut ou la réutilisation du matériel, il convient de vérifier si celui-ci contient ou non un support de stockage.

Il convient de détruire physiquement les supports de stockage contenant de l'information confidentielle ou protégée par le droit d'auteur, ou bien de détruire, supprimer ou écraser cette information en privilégiant les techniques rendant l'information d'origine irrécupérable plutôt qu'en utilisant la fonction standard de suppression ou de formatage. Voir 7.10 pour des recommandations détaillées sur la mise au rebut des supports de stockage et 8.10 pour des recommandations sur la suppression d'information.

Il convient de retirer les étiquettes et marquages qui identifient l'organisation ou indiquent la classification, le propriétaire, le système ou le réseau avant la mise au rebut, y compris en cas de revente ou de don à une organisation caritative.

Il convient que l'organisation envisage le retrait des mesures de sécurité telles que les contrôles d'accès ou le matériel de surveillance à l'expiration du bail ou lors de son déménagement. Cela dépend de facteurs tels que :

a) son contrat de location stipulant la remise de l'installation dans son état d'origine ;

b) la réduction au minimum du risque de laisser des systèmes contenant de l'information sensible aux mains du prochain locataire, qu'il s'agisse de listes d'accès des utilisateurs, de fichiers vidéo ou de fichiers images ;

c) la possibilité de réutiliser les mesures dans l'installation suivante.

Informations supplémentaires

Il peut être nécessaire de procéder à une appréciation du risque relatif au matériel endommagé contenant des supports de stockage pour déterminer s'il convient de le détruire physiquement plutôt que de le faire réparer ou de le mettre au rebut. L'information peut être compromise par une mise au rebut ou un recyclage du matériel effectué sans minutie.

En plus de sécuriser l'effacement des disques, le chiffrement intégral des disques réduit le risque de divulgation de l'information confidentielle lorsque le matériel est mis au rebut ou remis en service, pourvu que :

a) le processus de chiffrement soit suffisamment fort et couvre l'intégralité du disque (y compris les espaces perdus et les fichiers d'échange) ;

b) les clés cryptographiques soient suffisamment longues pour résister aux attaques par force brute ;

c) les clés cryptographiques soient elles-mêmes confidentielles (dans le sens où elles ne sont jamais stockées sur le même disque).

Pour des conseils plus détaillés sur la cryptographie, voir 8.24.

Les techniques d'écrasement sécurisé des supports de stockage diffèrent en fonction de la technologie du support de stockage et du niveau de classification de l'information stockée sur le support. Il convient de passer en revue les outils d'écrasement pour s'assurer qu'ils sont adaptés à la technologie du support de stockage considéré.

Voir l'ISO/IEC 27040 pour plus d'informations sur les méthodes de nettoyage des supports de stockage.

8 Mesures technologiques

8.1 Terminaux utilisateurs

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Protection

Mesure de sécurité

Il convient de protéger toute information stockée sur un terminal utilisateur final, traitée par ou accessible via ce type d'appareil.

Objectif

Protéger l'information contre les risques occasionnés par l'utilisation de terminaux utilisateurs.

Préconisations

Généralités

Il convient que l'organisation établisse une politique portant sur le thème de la configuration et de la manipulation sécurisées des terminaux utilisateurs finaux. Il convient de communiquer la politique portant sur un thème à tout le personnel concerné et de prendre en compte les points suivants :

a) le type d'information et le niveau de classification que les terminaux finaux peuvent prendre en charge, traiter ou supporter ;

b) enregistrement des terminaux utilisateurs finaux ;

c) exigences liées à la protection physique ;

d) restriction de l'installation de logiciel (par exemple, contrôlée à distance par les administrateurs système) ;

e) exigences relatives à la version du logiciel des terminaux utilisateurs et à l'application des mises à jour (par exemple, activation des mises à jour automatiques) ;

f) règles de connexion aux services d'information, aux réseaux publics ou à tout autre réseau en dehors des locaux (par exemple, exigeant l'utilisation du pare-feu personnel) ;

g) contrôles d'accès ;

h) chiffrement des dispositifs de stockage ;

i) protection contre les programmes malveillants, détection et réponse (par exemple, utilisation d'un logiciel de protection défini) ;

j) désactivation, suppression des données ou verrouillage à distance ;

k) sauvegardes ;

l) utilisation des services web et des applications web ;

m) analyse du comportement des utilisateurs finaux ;

n) utilisation de dispositifs de mémoire amovibles et possibilité de désactiver les ports USB ;

o) utilisation de fonctions de partitionnement, si le terminal final de l'utilisateur les prend en charge, pouvant séparer de façon sécurisée l'information et les autres actifs associés de l'organisation (par exemple, les logiciels) de l'information et des autres actifs associés présents sur l'appareil.

Dans la mesure du possible, il convient d'appliquer les recommandations de la présente mesure par le biais de la gestion de la configuration (voir 8.9) ou d'outils automatisés.

Responsabilité de l'utilisateur

Il convient que tous les utilisateurs soient sensibilisés aux exigences et aux procédures de sécurité destinées à protéger les terminaux utilisateurs, ainsi qu'aux responsabilités qui leur incombent pour assurer la mise en œuvre de cette protection. Il convient de recommander aux utilisateurs :

a) de se déconnecter des sessions actives et des services lorsqu'ils n'en ont plus besoin ;

b) lorsqu'ils ne s'en servent pas, de protéger les terminaux utilisateurs finaux contre toute utilisation non autorisée par le biais d'une serrure à clé ou d'un dispositif équivalent, tel qu'un accès par mot de passe ;

c) l'utilisation des appareils à adopter dans les lieux publics, les bureaux ouverts, les lieux de réunion et autres zones non protégées (par exemple, éviter de lire des informations confidentielles si des personnes peuvent lire derrière l'utilisateur ou utiliser des filtres d'écran).

Il convient que les terminaux soient physiquement protégés contre le vol ; par exemple, dans un véhicule privé ou tout autre moyen de transport, une chambre d'hôtel, un centre de congrès ou une salle de réunion. Il convient d'établir une procédure spécifique tenant compte des exigences légales, statutaires, réglementaires, contractuelles (y compris en matière d'assurance) et des autres exigences de sécurité de l'organisation, en cas de vol ou de perte de terminaux utilisateurs. Il convient de ne pas laisser sans surveillance les appareils dans lesquels sont stockées des informations importantes, sensibles ou critiques liées à l'activité de l'organisation et, si possible, de les mettre sous clé ou de les doter de systèmes de verrouillage spéciaux. Il convient de déterminer si certaines informations, de par leur caractère sensible, peuvent uniquement être consultées sur les terminaux utilisateurs finaux, mais pas y être stockées. Dans ce cas, des dispositifs de protection supplémentaires peuvent être exigés sur l'appareil. Il peut, par exemple, s'agir de s'assurer que le téléchargement de fichiers pour le travail en ligne soit désactivé, de même que le stockage local sur carte SD.

Utilisation d'appareils personnels

Lorsque l'organisation autorise l'utilisation d'appareils personnels (parfois désignée par l'acronyme AVEC pour « Apportez votre équipement personnel de communication »), en plus des éléments qui précèdent, il convient également de prendre en compte les exigences et mesures de sécurité correspondantes :

a) une séparation entre l'utilisation personnelle et l'utilisation professionnelle des appareils, impliquant la mise en œuvre d'un logiciel pour faciliter cette séparation et protéger les données liées à l'activité de l'organisation figurant sur un appareil privé ;

b) de ne permettre l'accès aux informations métier que lorsque l'utilisateur a reconnu les obligations qui lui incombent (protection physique, mise à jour des logiciels, etc.), renoncé à la propriété des données métier et autorisé l'organisation à effacer ses données à distance en cas de perte ou de vol de l'appareil, ou lorsque l'utilisation du service n'est plus autorisée. Cette politique portant sur un thème doit tenir compte de la législation en vigueur sur la protection des DCP ;

c) les politiques portant sur des thèmes et les procédures mises au point pour prévenir tout litige relatif aux droits de propriété intellectuelle sur des actifs créés sur un matériel détenu à titre privé ;

d) l'accès au matériel détenu à titre privé (pour vérifier le niveau de sécurité de la machine ou lors d'une enquête), susceptible d'être interdit par la loi ;

e) les contrats de licence logicielle pouvant rendre l'organisation responsable de l'octroi des licences pour les logiciels clients des terminaux utilisateurs détenus à titre privé par le personnel et des utilisateurs tiers.

Connexions sans fil

Il convient que l'organisation établisse des procédures pour :

a) la configuration des connexions sans fil sur les appareils (par exemple, désactivation des protocoles vulnérables) ;

b) la mise en œuvre de la connexion à des réseaux filaires ou sans fil rapides conformément à la politique portant sur le thème du contrôle d'accès (par exemple, si des sauvegardes ou des mises à jour logicielles sont nécessaires).

Informations supplémentaires

Généralement, les terminaux utilisateurs partagent des fonctions communes avec les terminaux utilisateurs fixes, par exemple les fonctions réseau, l'accès Internet, la messagerie électronique et le traitement des fichiers. Les mesures de sécurité de l'information liées aux terminaux utilisateurs finaux comprennent, généralement, les mesures adoptées dans le cadre de l'utilisation d'appareils fixes et les mesures destinées à traiter les menaces découlant de leur utilisation en dehors des locaux de l'organisation.

Les connexions sans fil des terminaux utilisateurs finaux reposent sur le même principe que les autres types de connexion réseau. Cependant, elles présentent des différences importantes qu'il convient de prendre en compte lors de la définition des mesures de sécurité. Différences typiques :

a) certains protocoles de sécurité sans fil sont en phase de rodage et leurs failles sont connues ;

b) la sauvegarde des informations stockées sur les terminaux utilisateurs finaux n'est pas toujours possible en raison d'une bande passante limitée ou parce que les appareils mobiles ne sont pas connectés au moment où les sauvegardes automatiques sont programmées.

8.2 Privilèges d'accès

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient de restreindre et de gérer l'attribution et l'utilisation des privilèges d'accès.

Objectif

S'assurer que seuls les utilisateurs autorisés, les composants logiciels et les services se voient attribuer des privilèges d'accès.

Préconisations

Il convient de contrôler l'attribution des privilèges d'accès par le biais d'une procédure d'autorisation, conformément à la politique portant sur le thème du contrôle d'accès (voir 5.15). Il convient de considérer les éléments suivants :

a) identifier les utilisateurs qui ont besoin de privilèges d'accès pour chaque système ou processus, par exemple les systèmes d'exploitation, systèmes de gestion de base de données et applications ;

b) attribuer des privilèges d'accès aux utilisateurs si besoin et au cas par cas, conformément à la politique portant sur le thème du contrôle d'accès (voir 5.15), c'est-à-dire en fonction de l'exigence minimale requise par leur rôle fonctionnel ;

c) tenir à jour une procédure d'autorisation et un enregistrement de tous les privilèges qui ont été attribués. Déterminer qui peut approuver les privilèges d'accès. N'accorder aucun privilège d'accès jusqu'à ce que la procédure d'autorisation soit achevée ;

d) définir et mettre en œuvre les exigences liées à l'expiration des privilèges d'accès ;

e) prendre des dispositions pour s'assurer que les utilisateurs connaissent leurs privilèges d'accès et sachent à quel moment ils passent en mode d'accès privilégié. L'utilisation d'une identité utilisateur spécifique, de paramètres d'interface utilisateur voire de matériel spécifique font partie des dispositions possibles ;

f) les exigences d'authentification relatives aux privilèges d'accès peuvent être plus fortes que les exigences relatives aux droits d'accès normaux. Une réauthentification ou une authentification supérieure peut s'avérer nécessaire pour pouvoir travailler avec des privilèges d'accès ;

g) régulièrement et après tout changement organisationnel, passer en revue les utilisateurs qui travaillent avec des privilèges d'accès pour vérifier si leurs missions, rôles, responsabilités et compétences justifient encore le fait qu'ils bénéficient de privilèges d'accès (voir 5.18) ;

h) attribuer des privilèges d'accès aux seules personnes disposant des compétences nécessaires ;

i) établir des règles spécifiques pour éviter l'utilisation d'identifiants utilisateurs d'administration génériques (tels que « root »), en fonction des possibilités de configuration des systèmes. Gérer et protéger les informations d'authentification de ces identités (voir 5.17) ;

j) accorder les privilèges d'accès seulement pour la période nécessaire à la mise en œuvre des changements approuvés, plutôt que d'accorder des privilèges d'accès de façon permanente ou d'accorder l'accès à des identités ayant des privilèges d'accès de façon continue. Cette procédure est souvent qualifiée de « bris de glace » et, dans la plupart des cas, automatisée par des technologies de gestion des privilèges d'accès ;

k) journaliser tous les accès administratifs au système à des fins d'audit ;

l) ne pas partager ni lier des identités présentant des privilèges d'accès ou des droits d'accès de niveau administrateur avec plusieurs personnes, attribuer à chaque personne une identité distincte permettant d'attribuer des privilèges d'accès spécifiques. Les identités peuvent être regroupées, par exemple en définissant un groupe d'administrateurs pour simplifier la gestion des privilèges d'accès ;

m) utiliser uniquement les identités ayant des privilèges d'accès ou des droits d'accès de niveau administrateur pour réaliser des tâches d'administration et non dans le cadre des tâches générales quotidiennes, telles que la consultation de la messagerie ou l'accès à Internet (il convient que les utilisateurs disposent d'une identité réseau normale distincte pour effectuer ces activités).

Informations supplémentaires

Les privilèges d'accès sont les droits d'accès accordés à un compte ou processus, et qui permettent à ce dernier d'effectuer des activités qu'un utilisateur ou processus standard ne peut effectuer. Le rôle qui bénéficie le plus couramment de privilèges d'accès est celui d'administrateur système.

Une mauvaise utilisation des privilèges d'administration système (toute fonction ou tout équipement d'un système d'information permettant de passer outre les contrôles de système ou d'application) peut constituer un facteur important de défaillance ou de violation des systèmes.

De plus amples informations sur la gestion des accès et la gestion sécurisée de l'accès à l'information et aux ressources des technologies d'information et de communication sont disponibles dans l'ISO/IEC 29146.

8.3 Restriction d'accès à l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient que l'accès à l'information et aux autres actifs associés soit restreint conformément à la politique portant sur le thème du contrôle d'accès.

Objectif

Garantir l'accès par le biais d'autorisations seulement et empêcher l'accès non autorisé à l'information et aux autres actifs associés.

Préconisations

Il convient que les restrictions d'accès à l'information et aux autres actifs associés soient basées sur les besoins de l'activité conformément à la politique portant sur le thème du contrôle d'accès (5.15).

Pour soutenir les exigences relatives aux restrictions d'accès, il convient d'envisager les points suivants :

a) l'information sensible en termes de confidentialité ne doit pas être accessible à des identités d'utilisateurs inconnues ni de façon anonyme. Il convient d'accorder une attention particulière aux emplacements de stockage qui autorisent les paramètres d'accès lisibles publiquement ;

b) fournir des mécanismes de configuration pour contrôler l'accès à l'information dans les systèmes, applications et services ;

c) contrôler les données auxquelles peut accéder un utilisateur donné ;

d) contrôler les identités ou le groupe d'identités qui bénéficient d'un accès donné, tel qu'en lecture, en écriture, en suppression et en exécution ;

e) mettre à disposition des contrôles d'accès physiques ou logiques permettant d'isoler les applications, les données des applications ou les systèmes sensibles.

Il convient également d'envisager des techniques et processus de gestion des accès dynamiques pour protéger l'information sensible qui possède une valeur élevée pour l'organisation lorsque cette dernière :

a) a besoin d'exercer un contrôle granulaire sur les utilisateurs qui peuvent accéder à ladite information durant une période définie et d'une façon déterminée ;

b) veut partager ladite information avec des personnes extérieures à l'organisation et déterminer qui sont les utilisateurs pouvant y accéder ;

c) veut gérer de façon dynamique, en temps réel, l'utilisation et la distribution de ladite information ;

d) veut protéger ladite information contre les modifications, la reproduction et la distribution (impression comprise) non autorisées ;

e) veut surveiller l'utilisation de l'information ;

f) veut enregistrer tout changement apporté à ladite information dans l'éventualité d'une future enquête.

Il convient que les techniques de gestion des accès dynamiques fournissent une protection tout au long du cycle de vie de l'information (création, traitement, stockage, transmission et destruction), y compris :

a) définition de règles relatives à la gestion de l'accès dynamique basées sur des cas d'utilisation spécifiques, en prenant en compte :

    1) l'attribution des autorisations d'accès par rapport à l'identité, au dispositif, à l'emplacement ou à l'application ;

    2) l'exploitation du plan de classification pour déterminer la nature de l'information qu'il est nécessaire de protéger à l'aide des techniques de gestion des accès dynamiques.

b) la mise en place de processus opérationnels, de surveillance de production de rapports ainsi que de l'infrastructure technique sous-jacente.

Il convient que les systèmes de gestion des accès dynamiques protègent l'information par les biais suivants :

a) exigent l'authentification, les justificatifs d'identité appropriés ou un certificat pour accéder à l'information ;

b) limitent l'accès, par exemple à une période définie (par exemple, après une date donnée ou jusqu'à une date donnée) ;

c) utilisent le chiffrement pour protéger l'information ;

d) définissent les autorisations d'impression de l'information ;

e) enregistrent l'identité des utilisateurs qui accèdent à l'information et son mode d'utilisation ;

f) émettent des alertes s'ils détectent des tentatives de mauvais usage de l'information.

Informations supplémentaires

Les techniques de gestion des accès dynamiques et d'autres technologies de protection de l'information dynamique peuvent prendre en charge la protection de l'information même si des données sont partagées au-delà de l'organisation d'origine, où les contrôles d'accès traditionnels ne peuvent pas être appliqués. Elles peuvent être appliquées à des documents, des courriers électroniques ou d'autres informations sur fichier, afin de limiter les utilisateurs pouvant accéder au contenu et les façons d'y accéder. Il peut s'agir d'un niveau granulaire qui peut être adapté tout au long du cycle de vie de l'information.

Les techniques de gestion des accès dynamiques ne remplacent pas la gestion des accès classique, par exemple l'utilisation de listes de contrôle d'accès, mais elles peuvent ajouter des facteurs de conditionnalité, d'évaluation en temps réel, de réduction des données à la volée et d'autres améliorations qui peuvent s'avérer bénéfiques pour l'information la plus sensible. Elles permettent de contrôler l'accès hors de l'environnement de l'organisation. La réponse aux incidents peut être prise en charge par les techniques de gestion des accès dynamiques dans la mesure où les autorisations peuvent être modifiées ou annulées à tout moment.

Des informations supplémentaires sont disponibles dans l'ISO/IEC 29146.

8.4 Accès au code source

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès #Sécurité_des_applications	#Protection

Mesure de sécurité

Il convient de gérer de façon appropriée l'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques logicielles.

Objectif

Empêcher l'introduction d'une fonctionnalité non autorisée, éviter toute modification involontaire ou malveillante et préserver la confidentialité de la propriété intellectuelle de valeur.

Préconisations

Il convient d'exercer un contrôle strict de l'accès au code source et aux éléments associés (tels que les exigences de conception, les spécifications, les programmes de vérification et de validation) et aux outils de développement (tels que les compilateurs, générateurs, outils d'intégration, plateformes et environnements de test).

En ce qui concerne le code source, ce contrôle peut prendre la forme d'un stockage centralisé du code, de préférence dans le système de gestion du code source.

L'accès en lecture et l'accès en écriture au code source peuvent différer en fonction du rôle du personnel. Par exemple, l'accès en lecture peut être disponible de façon générale dans l'organisation, tandis que l'accès en écriture est uniquement disponible pour des employés privilégiés ou des propriétaires désignés. Lorsque le code est réutilisé au sein d'une organisation, il convient de mettre en œuvre l'accès en lecture à un référentiel de code centralisé. En outre, si des éléments de code source libre ou de code tiers sont utilisés dans une organisation, l'accès en lecture à ces référentiels de code externes peut être ouvert au plus grand nombre. En revanche, il convient toujours de restreindre l'accès en écriture.

Il convient de prendre en compte les lignes directrices suivantes pour contrôler l'accès aux bibliothèques de code source en vue de réduire les risques d'altération des programmes informatiques :

a) gérer l'accès au code source du programme et aux bibliothèques de programmes sources conformément aux procédures établies ;

b) attribuer l'accès en lecture et en écriture au code source en fonction des besoins de l'activité et gérer ce dernier en vue de traiter les risques d'altération ou de mauvais usage et conformément aux procédures établies ;

c) mettre à jour le code source et les éléments associés et attribuer l'accès au code source conformément aux procédures de contrôle des changements (voir 8.32) et y accéder uniquement après avoir reçu l'autorisation appropriée ;

d) ne pas accorder aux développeurs un accès direct au code source, mais par l'intermédiaire d'outils de développement qui contrôlent les activités et les autorisations relatives au code source ;

e) stocker des listings des programmes dans un environnement sécurisé où il convient de gérer l'accès en lecture et en écriture de façon appropriée ;

f) tenir un journal d'audit de tous les accès et de toutes les modifications apportées au code source.

Si le code source du programme est destiné à être publié, il convient d'envisager des mesures supplémentaires pour apporter l'assurance de son intégrité (par exemple, une signature électronique).

Informations supplémentaires

Aucune autre information.

8.5 Authentification sécurisée

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Mesure de sécurité

Il convient de mettre en œuvre des technologies et procédures d'authentification sécurisée sur la base des restrictions d'accès à l'information et de la politique portant sur le thème du contrôle d'accès.

Objectif

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

Préconisations

Il convient de choisir une technique d'authentification permettant de vérifier l'identité déclarée par un utilisateur, un logiciel, des messages et autres entités.

Il convient d'adapter le niveau d'authentification en fonction de la classification de l'information à consulter. Lorsqu'un niveau élevé d'authentification et d'identification est requis, il convient d'utiliser des méthodes d'authentification autres que l'utilisation de mots de passe, par exemple un procédé cryptographique, des certificats numériques, des cartes à puce, des jetons d'authentification ou des techniques de biométrie.

Il convient que les facteurs d'authentification soient accompagnés par des facteurs d'authentification supplémentaires pour l'accès aux systèmes d'information critiques (principe également désigné sous le nom « d'authentification multifactorielle »). Le fait de conjuguer plusieurs facteurs d'authentification, par exemple ce que vous savez, ce que vous avez et ce que vous êtes, limite les possibilités d'accès non autorisé. L'authentification multifactorielle peut être associée à d'autres techniques pour exiger des facteurs additionnels dans des circonstances précises, en fonction de règles et de modèles prédéfinis ; par exemple lieu inhabituel, dispositif inhabituel ou heure inhabituelle.

Il convient d'invalider les informations d'authentification biométrique si jamais elles sont compromises. L'authentification biométrique peut être indisponible selon les conditions d'utilisation (par exemple, humidité ou ancienneté). Pour anticiper ce type de problème, il convient d'adjoindre à l'authentification biométrique au moins une technique d'authentification alternative.

Il convient que la procédure de connexion à un système ou à une application soit conçue de manière à réduire au minimum les risques d'accès non autorisé. Par conséquent, il convient que cette procédure de connexion ne dévoile qu'un minimum d'information sur le système ou l'application, afin d'éviter de faciliter la tâche d'un éventuel utilisateur non autorisé. Il convient de mettre en œuvre les procédures et technologies de connexion en tenant compte des éléments suivants :

a) ne pas afficher d'information sensible sur le système ou l'application tant que le processus de connexion n'est pas terminé ;

b) afficher un avertissement précisant qu'il convient que l'accès au système, à l'application ou au service soit réservé aux seuls utilisateurs autorisés ;

c) ne pas proposer, pendant la procédure de connexion, de messages d'aide qui pourraient faciliter un accès non autorisé (si une condition d'erreur survient, il convient que le système n'indique pas quelle partie des données est correcte ou incorrecte) ;

d) valider l'information de connexion seulement lorsque toutes les données d'entrée ont été saisies ;

e) se protéger contre les tentatives de connexion par force brute sur les noms d'utilisateurs et mots de passe (par exemple, utilisation de code captcha, exigence de réinitialisation du mot de passe au bout d'un nombre de tentatives défini ou blocage de l'utilisateur après un nombre d'erreurs maximal) ;

f) enregistrer les tentatives réussies et avortées ;

g) lancer une alerte de sécurité en cas de détection d'une brèche possible, réussie ou avortée, dans les contrôles de connexion (par exemple, lancer une alerte adressée à l'utilisateur et aux administrateurs système de l'organisation lorsqu'un certain nombre de tentatives de saisie du mot de passe est atteint) ;

h) afficher ou envoyer les informations suivantes sur un canal distinct après une connexion réussie :

   1) la date et l'heure de la dernière connexion réussie ;

   2) les détails relatifs à toute tentative de connexion avortée depuis la dernière tentative réussie ;

i) ne pas afficher le mot de passe en texte clair pendant sa saisie ;

j) ne pas transmettre les mots de passe en texte clair sur un réseau pour éviter qu'ils ne soient récupérés par un programme « renifleur » de réseau ;

k) mettre fin aux sessions inactives au bout d'une période définie d'inactivité, notamment dans les endroits présentant des risques élevés, comme les lieux publics ou à l'extérieur des locaux soumis au management de la sécurité de l'organisation, ou sur les terminaux utilisateurs ;

l) restreindre les durées de connexion pour apporter une sécurité supplémentaire aux applications à haut risque et réduire les risques de tentatives d'accès non autorisé.

Informations supplémentaires

D'autres informations sur l'assurance de l'authentification d'entité sont disponibles dans l'ISO/IEC 29115.

8.6 Dimensionnement

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Disponibilité	#Identification #Protection #Détection	#Continuité	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient de surveiller l'utilisation des ressources et de l'ajuster conformément au dimensionnement actuel et prévu.

Objectif

Garantir la disponibilité requise des moyens de traitement de l'information.

Préconisations

Il convient d'identifier le dimensionnement des moyens de traitement de l'information, des ressources humaines, des bureaux et autres installations, en tenant compte du caractère critique pour l'activité des systèmes et processus concernés.

Il convient d'appliquer un ajustement au plus près et une surveillance des systèmes pour assurer, et s'il y a lieu améliorer, leur disponibilité et leur efficacité.

Il convient de mettre en place des mesures de détection pour identifier les problèmes en temps voulu.

Il convient que les projections en matière de dimensionnement futur tiennent compte des nouvelles exigences métier et système, et des orientations présentes et projetées de l'organisation en matière de capacité de traitement de l'information.

Il convient de porter une attention particulière aux ressources pour lesquelles les délais d'approvisionnement sont longs ou les coûts élevés : il convient donc que les responsables et les propriétaires de produits ou services surveillent l'utilisation des ressources clés du système.

Il convient que les responsables utilisent l'information relative aux capacités pour identifier et éviter les limitations de ressources potentielles, et pour éviter d'avoir à dépendre de personnel clé, ce qui peut représenter une menace pour la sécurité du système ou pour les services, et qu'ils planifient l'action appropriée.

Il est possible d'atteindre un dimensionnement suffisant en augmentant la capacité du système ou en réduisant la demande.

Il convient d'envisager les points suivants pour augmenter la capacité :

a) embauche de nouveau personnel ;

b) obtention de nouvelles installations ou d'espace supplémentaire ;

c) acquisition de systèmes de traitement plus puissants, de mémoire et de stockage supplémentaires ;

d) recours à l'informatique en nuage, dont les caractéristiques répondent directement aux problèmes de capacité. L'informatique en nuage possède l'élasticité et l'évolutivité nécessaires pour permettre l'expansion et la réduction rapides à la demande des ressources disponibles. Pour des applications et services définis.

Il convient de prendre en compte les éléments suivants pour réduire la demande qui pèse sur les ressources de l'organisation :

a) suppression des données obsolètes (espace disque) ;

b) élimination des copies papier qui ont atteint leur durée de conservation (libération d'espace sur les rayonnages) ;

c) mise hors service d'applications, de systèmes, de bases de données ou d'environnements ;

d) optimisation des traitements par lots et de la planification ;

e) optimisation de la logique des applications ou des requêtes de bases de données ;

f) refus des services gourmands en ressources ou limitation de la bande passante, si ceux-ci ne sont pas considérés comme critiques (par exemple, les retransmissions vidéo).

Il convient d'étudier un plan documenté de la gestion du dimensionnement pour les systèmes critiques.

Informations supplémentaires

Pour plus de détails sur l'élasticité et l'évolutivité de l'informatique en nuage, voir l'ISO/IEC TS 23167.

8.7 Protection contre les programmes malveillants

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection #Défense

Mesure de sécurité

Il convient de mettre en œuvre une protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés.

Objectif

Veiller à ce que l'information et les autres actifs associés soient protégés contre les programmes malveillants.

Préconisations

Il convient que la protection contre les programmes malveillants soit fondée sur des logiciels de détection des programmes malveillants et de réparation, la sensibilisation à la sécurité de l'information, et des mesures adéquates de gestion des changements et d'accès au système. La simple utilisation de logiciels de détection et de réparation n'est généralement pas suffisante. Il convient d'envisager les préconisations suivantes :

a) mettre en œuvre des mesures destinées à empêcher ou à détecter l'utilisation de logiciels non autorisés (par exemple, liste d'autorisation des applications, c'est-à-dire recours à une liste indiquant les applications autorisées) (voir 8.19 et 8.32) ;

b) mettre en œuvre des mesures destinées à empêcher ou à détecter l'utilisation de sites Web connus pour leur caractère malveillant ou suspectés en tant que tels (par exemple, liste de blocage) ;

c) réduire les vulnérabilités pouvant être exploitées par des programmes malveillants, par exemple grâce à une gestion des vulnérabilités techniques (voir 8.8 et 8.19) ;

d) procéder à une validation automatique régulière des logiciels et du contenu de données des systèmes qui gèrent les processus métier critiques ; mener des investigations sur la présence de fichiers non approuvés ou de modifications non autorisées ;

e) mettre en place des mesures de protection contre les risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via des réseaux externes que sur tout autre support ;

f) procéder à l'installation et à la mise à jour régulière de logiciels de détection des programmes malveillants et de réparation pour analyser les ordinateurs et les supports ; exécuter une analyse qui englobe :

   1) une analyse de tout fichier reçu sur les réseaux ou via toute forme de support de stockage, pour s'assurer de l'absence de programme malveillant avant utilisation ;

   2) une analyse des pièces jointes aux courriers électroniques et aux messages instantanés, et des fichiers téléchargés pour s'assurer de l'absence de programme malveillant avant utilisation ; mener cette analyse en différents endroits, par exemple sur les serveurs de messagerie électronique, les ordinateurs de bureau et lors de l'accès au réseau de l'organisation ;

   3) une analyse lors de l'accès aux pages Web pour s'assurer de l'absence de programme malveillant ;

g) détermination du positionnement et de la configuration des outils de détection des programmes malveillants et de réparation par rapport aux résultats de l'appréciation du risque et en tenant compte des éléments suivants :

   1) principes de défense en profondeur et endroits où ils seraient les plus efficaces. Il peut, par exemple, s'agir de détecter les programmes malveillants au niveau d'une passerelle réseau (dans différents protocoles d'application tels que courrier électronique, transfert de fichiers et Internet) ainsi que des terminaux utilisateurs et des serveurs ;

   2) techniques d'évitement des attaquants, par exemple utilisation de fichiers chiffrés pour introduire des programmes malveillants ou recours à des protocoles chiffrés pour transmettre ces mêmes programmes ;

h) veiller à se protéger de l'introduction de programmes malveillants au cours des procédures de maintenance et d'urgence, qui peuvent contourner les mesures de protection habituelles ;

i) mettre en œuvre un processus permettant d'autoriser la désactivation temporaire ou permanente d'une partie ou de la totalité des mesures à l'encontre des programmes malveillants, notamment autorités d'agrément des exceptions, justification documentée et date de revue. Cela peut s'avérer nécessaire lorsque la protection contre les programmes malveillants entraîne une perturbation des activités habituelles ;

j) élaborer des plans de continuité d'activité en vue de la récupération après une attaque par programme malveillant, comprenant la sauvegarde de tous les logiciels et données nécessaires (sauvegarde en ligne aussi bien qu'hors ligne) et les dispositions de récupération (voir 8.13) ;

k) isoler les environnements au sein desquels les conséquences peuvent s'avérer désastreuses ;

l) définir des procédures et des responsabilités pour assurer la protection des systèmes contre les programmes malveillants, y compris la formation à l'utilisation de ces systèmes, le signalement et la récupération après une attaque par des programmes malveillants ; sensibilisation ou formation (voir 6.3) de tous les utilisateurs sur la façon d'identifier et, le cas échéant, d'atténuer la réception, l'envoi ou l'installation de courriers électroniques, fichiers ou programmes infectés par des programmes malveillants (l'information recueillie en n) et o) peut être utilisée pour assurer la mise à jour continue de la sensibilisation et de la formation) ;

m) mettre en œuvre des procédures pour recueillir régulièrement de l'information sur les nouveaux programmes malveillants, comme l'inscription à des listes de diffusion ou la consultation de sites Web pertinents ;

n) vérifier que l'information en rapport avec les programmes malveillants, comme les bulletins d'alerte, provient de sources qualifiées et réputées (par exemples, sites Internet fiables ou éditeurs de logiciels de protection contre les programmes malveillants) et qu'elle est exacte et informative.

Informations supplémentaires

Il peut ne pas être possible d'installer un logiciel de protection contre les programmes malveillants sur certains systèmes (tels que des systèmes de contrôle industriel).

Certains types de programmes malveillants infectent les systèmes d'exploitation des ordinateurs et leurs microprogrammes, de sorte que les mesures courantes de protection contre les programmes malveillants ne peuvent pas nettoyer le système et qu'une réinitialisation complète du logiciel d'exploitation et, parfois, du microgramme est nécessaire pour revenir à un état sûr.

8.8 Gestion des vulnérabilités techniques

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_menaces_et_des_vulnérabilités	#Gouvernance_et_écosystème #Protection #Défense

Mesure de sécurité

Il convient d'obtenir des informations sur les vulnérabilités techniques des systèmes d'information, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les mesures appropriées.

Objectif

Empêcher toute exploitation des vulnérabilités techniques.

Préconisations

Identification des vulnérabilités techniques

Dès l'identification de vulnérabilités techniques potentielles, il convient d'engager l'action appropriée dans les meilleurs délais ; réaliser un inventaire précis des actifs (voir 5.9 à 5.14) comme prérequis pour une gestion efficace des vulnérabilités techniques ; il convient que l'inventaire mentionne l'éditeur du logiciel, les numéros de versions, l'état actuel du déploiement (par exemple, nature du logiciel installé sur des systèmes définis) et la ou les personnes au sein de l'organisation qui sont responsables du logiciel.

Il convient d'envisager les préconisations suivantes pour identifier les vulnérabilités techniques :

a) définir et établir les rôles et les responsabilités associés à la gestion des vulnérabilités techniques, notamment la veille en matière de vulnérabilités, l'appréciation du risque correspondant, les mises à jour, le suivi des actifs, ainsi que toute responsabilité de coordination requise ;

b) pour les logiciels et autres technologies (en fonction de l'inventaire des actifs, voir 5.9), déterminer les ressources d'information permettant d'identifier les vulnérabilités techniques pertinentes et de sensibiliser les intervenants sur ces vulnérabilités ; tenir à jour la liste des ressources d'information par rapport aux changements effectués dans l'inventaire ou lorsque des ressources nouvelles ou utiles sont identifiées ;

c) demander aux fournisseurs de systèmes d'information (et des composants correspondants) d'assurer le signalement des vulnérabilités, leur traitement et leur divulgation ; y compris les exigences liées aux contrats applicables (voir 5.20) ;

d) utiliser les outils d'analyse des vulnérabilités adaptés aux technologies employées pour identifier les vulnérabilités et vérifier si l'application de correctifs visant à résoudre les vulnérabilités a abouti ;

e) faire réaliser des tests de pénétration planifiés, documentés et pouvant être répétés ou des évaluations des vulnérabilités par les personnes compétentes et autorisées pour permettre l'identification des vulnérabilités ; prendre des précautions dans la mesure où ces activités peuvent entraîner une compromission de la sécurité du système ;

f) suivre l'utilisation de bibliothèques tierces et de code source externe pour les vulnérabilités. Il convient d'intégrer ce point dans le codage sécurisé (voir 8.28).

Il convient que l'organisation élabore des procédures et développe la capacité à :

a) détecter l'existence de vulnérabilités dans ses produits et services, en tenant compte des éventuels composants externes qui y sont utilisés ;

b) recevoir des signalements de vulnérabilités de la part de sources internes ou externes ;

c) analyser et vérifier les signalements pour déterminer l'activité de réponse et de correction nécessaire ;

d) élaborer une action corrective (généralement, application de mises à jour ou de correctifs logiciels) ;

e) réaliser des tests pour valider l'efficacité de la correction ou de l'atténuation des risques ;

f) proposer des mécanismes permettant de vérifier l'authenticité de la correction.

Il convient que l'organisation mette à disposition un point de contact public dans le cadre de sa politique portant sur le thème de la divulgation des vulnérabilités afin que les chercheurs et autres personnes puissent signaler les problèmes. Il convient que les organisations mettent en place des procédures de signalement des vulnérabilités, telles que des programmes de prime au bogue (consistant à proposer des récompenses sous forme d'incitation à aider les organisations à identifier les vulnérabilités pour leur apporter la correction voulue), des formulaires de signalement en ligne et qu'elles tirent parti de l'intelligence des menaces ou des forums de partage d'informations appropriés. Il convient que l'organisation partage également des informations avec les organismes sectoriels compétents.

Évaluation des vulnérabilités techniques

Pour évaluer les vulnérabilités techniques identifiées, il convient d'envisager les préconisations suivantes :

a) définir un délai de réaction aux notifications relatives aux éventuelles vulnérabilités techniques pertinentes ;

b) lorsqu'une vulnérabilité technique potentielle est identifiée, déterminer les risques associés et les actions à entreprendre ; cela peut consister à mettre à jour les systèmes vulnérables ou à appliquer d'autres mesures ;

c) en fonction du caractère d'urgence présenté par la vulnérabilité technique, entreprendre l'action conformément aux mesures de gestion des changements (voir 8.32) ou en appliquant les procédures de réponse aux incidents liés à la sécurité de l'information suivantes (voir 5.26) ;

d) utiliser uniquement des mises à jour provenant de sources autorisées (qui peuvent être internes ou externes à l'organisation) ; si une mise à jour est disponible, évaluer les risques associés à l'installation de cette mise à jour (il convient de comparer les risques découlant de la vulnérabilité aux risques associés à l'installation de la mise à jour) ;

e) tester et évaluer les mises à jour avant de les installer afin de s'assurer de leur efficacité et de l'absence d'effets collatéraux ne pouvant pas être tolérés.

Prise des mesures appropriées pour répondre aux vulnérabilités techniques

Il convient de mettre en œuvre une politique de gestion des mises à jour afin que tous les logiciels autorisés bénéficient des toutes dernières versions des mises à jour d'applications et des correctifs logiciels approuvés. Lorsque des changements s'avèrent nécessaires, il convient de conserver le logiciel original et d'appliquer ces changements à une copie clairement identifiée. Il convient de tester avec soin et de documenter tous les changements apportés afin de pouvoir les réappliquer aux versions ultérieures, le cas échéant. Si nécessaire, il convient que les changements apportés soient testés et validés par un organisme indépendant.

Il convient d'envisager les préconisations suivantes pour répondre aux vulnérabilités techniques :

a) traiter en priorité les systèmes à haut risque ;

b) si aucune mise à jour n'est disponible ou que la mise à jour ne peut pas être installée, envisager d'autres mesures, telles que :

    1) l'application de toute solution de contournement proposée par l'éditeur du logiciel ou d'autres sources pertinentes ;

    2) la désactivation des services ou des fonctions liés à la vulnérabilité ;

    3) l'adaptation ou l'ajout de contrôles d'accès, par exemple des pare-feu, aux limites du réseau (voir 8.20 à 8.23) ;

    4) la protection des systèmes, dispositifs ou applications vulnérables contre toute attaque grâce au déploiement de filtres de trafic adaptés (parfois appelée « application de correctifs virtuels ») ;

    5) le renforcement du dispositif de surveillance visant à détecter les attaques réelles ;

    6) le renforcement de la politique de sensibilisation aux vulnérabilités.

Si les éditeurs des logiciels achetés publient régulièrement des informations sur leurs mises à jour de sécurité et proposent un moyen pour installer automatiquement lesdites mises à jour, il convient que l'organisation décide d'utiliser ou non le système de mise à jour automatique.

Autres éléments à prendre en considération

Il convient de tenir un journal d'audit de toutes les étapes entreprises.

Il convient de surveiller et d'évaluer à intervalles réguliers le processus de gestion des vulnérabilités techniques afin de s'assurer de son efficacité.

Il convient d'harmoniser les activités de gestion des incidents avec un processus efficace de gestion des vulnérabilités techniques, pour communiquer les données relatives aux vulnérabilités à la fonction de réponse aux incidents et fournir des procédures techniques à exécuter en cas d'incident.

Si l'organisation utilise un système d'informatique en nuage mis à disposition par un fournisseur de services en nuage tiers, il incombe à ce fournisseur de gérer les vulnérabilités techniques de ses propres ressources. Il convient que les responsabilités du fournisseur de services en nuage en matière de gestion des vulnérabilités techniques soient intégrées à l'accord relatif aux services en nuage et que celui-ci précise les procédures de signalement des actions du fournisseur de services en nuage concernant les vulnérabilités techniques (voir 5.23). Pour certains services en nuage, les responsabilités sont divisées entre le fournisseur de services en nuage et le client de services en nuage. Le client de services en nuage est responsable de la gestion des vulnérabilités liées à ses actifs.

Informations supplémentaires

La gestion des vulnérabilités techniques peut être considérée comme une sous-fonction de la gestion des changements et peut, de ce fait, bénéficier des mêmes processus et procédures (voir 8.32).

Les éditeurs sont souvent soumis à d'importantes pressions pour publier les mises à jour au plus tôt. Il peut donc arriver qu'une mise à jour ne traite pas le problème de manière adéquate et qu'elle produise des effets collatéraux indésirables. De plus, dans certains cas, il peut être difficile de désinstaller une mise à jour une fois qu'elle a été appliquée.

S'il n'est pas possible de tester correctement les mises à jour, par exemple pour des raisons de coût ou par manque de ressources, l'application de la mise à jour peut être repoussée à une date ultérieure, le temps d'évaluer les risques associés en s'appuyant sur l'expérience d'autres utilisateurs. L'utilisation de l'ISO/IEC 27031 peut s'avérer utile.

L'une des raisons de ne pas opter pour les mises à jour automatiques est de conserver le contrôle sur la date d'application de la mise à jour. Par exemple, si un programme qui tourne sur un serveur demande 72 heures pour arriver à son terme, la mise à jour de ce serveur ne pourra être effectuée qu'une fois l'exécution du programme achevée, faute de quoi elle devra être relancée.

Les tests de pénétration permettent également d'identifier les vulnérabilités. Effectués dans les règles, ils peuvent identifier les vulnérabilités liées à l'ingénierie sociale aussi bien que les vulnérabilités techniques.

L'analyse des vulnérabilités présente un point faible dans le sens où elle peut ne pas totalement intégrer la défense en profondeur : deux contre-mesures qui sont toujours appelées dans le même ordre peuvent comporter des vulnérabilités qui sont masquées par les points forts de l'autre. La contre-mesure composite n'est pas vulnérable, alors qu'un programme d'analyse des vulnérabilités peut signaler que les deux composantes sont vulnérables. Il convient donc que les organisations se montrent prudentes lorsqu'elles passent en revue et traitent les signalements de vulnérabilités.

L'étiquette d'identification du logiciel (SWID) permet une gestion des vulnérabilités techniques plus poussée. Elle peut fournir des informations probantes et authentifiées sur la provenance du logiciel et, le cas échéant, inclure toutes les informations du manifeste, ce qui permet d'appliquer des mesures de sécurité basées sur les listes d'autorisation et pas uniquement les listes de blocage. Elle permet également d'accéder à des bases de données de vulnérabilités. Voir l'ISO/IEC 19770-2 pour de plus amples informations.

De nombreuses organisations fournissent des logiciels, systèmes, produits et services non seulement au sein de l'organisation, mais aussi à certaines parties intéressées telles que les clients, partenaires ou des utilisateurs tiers. Ces logiciels, systèmes, produits et services peuvent comporter des vulnérabilités en termes de sécurité de l'information se traduisant par des conséquences sur la sécurité des utilisateurs.

Dans le cadre du traitement de la divulgation, ces organisations peuvent publier une remédiation, divulguer les informations relatives aux vulnérabilités aux utilisateurs (généralement par l'intermédiaire d'un bulletin de sécurité public) et fournir les informations appropriées pour les services de base de données liés aux vulnérabilités des logiciels.

Si des correctifs logiciels ou des mises à jour sont produits, l'organisation peut envisager de mettre en œuvre un processus de mise à jour automatisé qui lancera l'installation de ces mises à jour sur les systèmes ou produits affectés sans que le client ou l'utilisateur ait besoin d'intervenir. Un processus de mise à jour automatisé peut permettre au client ou à l'utilisateur de sélectionner une option pour désactiver la mise à jour automatique ou contrôler le moment auquel sera effectuée l'installation de la mise à jour.

Plus de plus amples informations sur la gestion des vulnérabilités techniques dans le cadre de l'informatique en nuage, voir l'ISO/IEC 19086 (toutes les parties) et l'ISO/IEC 27017.

L'ISO/IEC 29147 propose des informations détaillées sur la réception de signalements de vulnérabilités et la publication de bulletins de sécurité sur les vulnérabilités. L'ISO/IEC 30111 propose des informations détaillées sur le traitement et la résolution des vulnérabilités signalées.

Pour réduire le nombre et l'impact des vulnérabilités, les organisations peuvent suivre les prescriptions 8.25 à 8.29 pour les activités de développement de logiciel liées aux produits et services à la fois au sein de l'organisation et pour le bénéfice de tiers.

8.9 Gestion de la configuration

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Configuration_sécurisée	#Protection

Mesure de sécurité

Il convient de définir, de documenter, de mettre en œuvre, de surveiller et réviser les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux.

Objectif

S'assurer du bon fonctionnement du matériel, des logiciels, des services et des réseaux avec les paramètres de sécurité requis, et du fait que la configuration ne soit pas altérée par des changements non autorisés ou incorrects.

Préconisations

Il convient que la configuration du matériel, des logiciels, des services (par exemple, services en nuage) et des réseaux soit soumise aux pratiques de management de la sécurité standard.

Il convient de définir des modèles standard pour la configuration de la sécurité du matériel, des logiciels, des services et des réseaux :

a) à l'aide des recommandations à la disposition du public, par exemple les modèles prédéfinis des éditeurs et des organismes de sécurité indépendants ;

b) en tenant compte du niveau de protection nécessaire pour déterminer un niveau de sécurité suffisant ;

c) prenant en charge la politique de sécurité de l'information de l'organisation, ses politiques portant sur des thèmes, les normes et les autres exigences en matière de sécurité ;

d) en envisageant la faisabilité et l'applicabilité des configurations de sécurité dans le contexte de l'organisation.

Il convient de réviser les modèles régulièrement et de les mettre à jour lorsqu'il est nécessaire de répondre à de nouvelles menaces ou vulnérabilités, ou lors de l'introduction de nouvelles versions du matériel ou des logiciels.

Il convient de mettre en place des rôles, responsabilités et procédures pour assurer un contrôle satisfaisant de tous les changements apportés.

Il convient de considérer les éléments suivants pour définir des modèles standard en vue de la configuration sécurisée du matériel, des logiciels et des services :

a) réduire au strict minimum le nombre d'identités dotées de privilèges d'accès ou de droits d'accès de niveau administrateur ;

b) désactiver les identités inutiles, non utilisées ou non sécurisées ;

c) désactiver ou restreindre les fonctions et services non nécessaires ;

d) restreindre l'accès aux programmes utilitaires puissants et au paramétrage des hôtes ;

e) synchroniser les horloges ;

f) modifier les informations d'authentification par défaut de l'éditeur, comme les mots de passe par défaut, immédiatement après l'installation et passer en revue les autres paramètres de sécurité par défaut importants ;

g) accéder aux moyens de délai d'attente qui déconnectent automatiquement les dispositifs de traitement informatique à l'issue d'une période d'inactivité prédéfinie ;

h) vérifier que les exigences liées à l'octroi de licences sont respectées (voir 5.32).

Il convient de consigner les configurations définies et de tenir un journal sur tous les changements de configuration. Il convient de stocker les documents correspondants de façon sécurisée. Ce principe peut être mis en œuvre de plusieurs façons, par exemple avec des bases de données ou des modèles de configuration.

Il convient que les changements apportés aux configurations suivent le processus de gestion des changements (voir 8.32).

Il convient que chaque document en appui de la gestion de la configuration, si disponible, contienne :

a) le propriétaire ou point de contact de chaque actif, qui doit être tenu à jour ;

b) les personnes responsables de la gestion de la configuration ;

c) la date d'approbation et de mise en œuvre de la configuration ;

d) la date ou la fréquence de révision de la configuration ;

e) les autres configurations associées et leur relation.

Il convient que l'organisation définisse et mette en œuvre les processus et outils nécessaires pour appliquer la configuration de sécurité définie aux nouveaux systèmes installés ainsi qu'aux systèmes opérationnels tout au long de leur durée de vie. Il convient de surveiller les configurations avec un ensemble exhaustif d'outils de gestion du système (par exemple, utilitaires de maintenance, assistance à distance, outils de gestion pour entreprise et logiciel de sauvegarde) et de les passer en revue régulièrement pour vérifier les paramètres de configuration, évaluer la force des mots de passe et les activités effectuées. Les configurations réelles peuvent être comparées aux modèles cibles définis. Il convient de traiter toute divergence, soit par une application automatique de la configuration cible définie, soit par analyse manuelle de la divergence suivie d'actions correctives.

Informations supplémentaires

La documentation des systèmes recèle souvent des détails relatifs au matériel et aux logiciels.

Le renforcement de la sécurité du système est une partie habituelle de la gestion de la configuration.

La gestion de la configuration peut être intégrée aux processus de gestion des actifs et aux outils associés, tels que la base de données de gestion des configurations (CMDB).

L'automatisation est généralement plus efficace pour gérer la configuration de la sécurité, par exemple à l'aide de « l'infrastructure en tant que code » (ou IaC pour Infrastructure as Code).

Les modèles et cibles de configuration peuvent constituer des informations confidentielles qu'il convient de protéger en conséquence contre tout accès non autorisé.

8.10 Suppression d'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité	#Protection	#Protection_des_informations	#Protection

Mesure de sécurité

Il convient de supprimer l'information stockée dans les systèmes d'information et les dispositifs lorsqu'elle n'est plus utile.

Objectif

Éviter l'exposition inutile d'information sensible et se conformer aux exigences légales, statutaires, réglementaires et contractuelles en matière de suppression de données.

Préconisations

Généralités

Il convient de ne pas conserver l'information sensible plus longtemps que nécessaire afin de réduire les risques de divulgation.

Lors de la suppression d'information au niveau de systèmes, d'applications et de services, il convient de prendre en compte les éléments suivants :

a) sélectionner une méthode de suppression conforme aux exigences métier et aux lois et réglementations en vigueur, par exemple : écrasement électronique ou brouillage à l'aide de la cryptographie ;

b) consigner les résultats de la suppression à titre de preuve ;

c) en cas de recours à des fournisseurs de services de suppression d'information, obtenir une preuve de la suppression d'information de la part des fournisseurs de services.

Lorsque de tierces parties traitent ou stockent l'information de l'organisation pour le compte de cette dernière, il convient que l'organisation veille à préciser les exigences liées à la suppression d'information dans les accords avec les tiers à appliquer lors de l'expiration de ces accords.

Méthodes de suppression

Conformément à la politique de l'organisation portant sur le thème de la conservation des données et compte tenu de la législation et des réglementations pertinentes, il convient de supprimer l'information sensible qui n'est plus utile par les moyens suivants :

a) configuration des systèmes en vue de la destruction sécurisée de l'information qui n'est plus utile (par exemple, à l'issue d'une période définie soumise à la politique portant sur le thème de la conservation des données ou via une demande d'accès aux informations personnelles) ;

b) suppression des versions, copies et fichiers temporaires obsolètes, quel que soit leur emplacement ;

c) utilisation de logiciels de suppression sécurisée agréés pour supprimer définitivement les données et contribuer à garantir que l'information ne puisse pas être récupérée à l'aide d'outils de récupération spécialisés ou d'outils scientifiques ;

d) recours à des prestataires de services de suppression sécurisée agréés et certifiés ;

e) recours à des mécanismes d'élimination adaptés au type de support à mettre au rebut, par exemple démagnétisation des disques durs et autres supports magnétiques.

Si l'organisation utilise des services en nuage, il convient qu'elle vérifie si la méthode de suppression disponible par l'intermédiaire du fournisseur de services en nuage est acceptable et, dans l'affirmative, que l'organisation l'utilise elle-même ou qu'elle demande au fournisseur de services en nuage de supprimer l'information. Il convient que ces processus de suppression soient automatisés conformément aux politiques portant sur des thèmes, si ces dernières sont disponibles et applicables. Selon la sensibilité des données supprimées, des journaux peuvent permettre de suivre les processus de suppression ou de vérifier qu'ils sont bien intervenus.

Pour éviter l'exposition involontaire de l'information sensible lorsque du matériel est renvoyé aux fournisseurs, il convient de protéger l'information sensible en retirant les dispositifs de stockage auxiliaire (comme les disques durs) et de mémoire avant que le matériel ne quitte les locaux de l'organisation. Il convient d'appliquer les mesures de contrôle décrites en 7.14 pour détruire physiquement le dispositif de stockage et supprimer simultanément l'information qu'il contient.

Un document officiel de suppression de l'information s'avère utile lors de l'analyse de la cause d'un possible événement de fuite d'information.

Informations supplémentaires

Des informations relatives à la suppression des données utilisateur dans les services en nuage sont disponibles dans l'ISO/IEC 27017.

8.11 Masquage des données

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité	#Protection	#Protection_des_informations	#Protection

Mesure de sécurité

Il convient d'utiliser le masquage des données conformément à la politique de l'organisation portant sur le thème du contrôle d'accès et aux exigences métier, tout en prenant en compte les exigences d'ordre légal.

Objectif

Limiter l'exposition de données sensibles, notamment les données à caractère personnel, et se conformer aux exigences légales, statutaires, réglementaires et contractuelles.

Préconisations

Lorsque la protection des données sensibles, telles que les données à caractère personnel, revêt de l'importance, il convient que l'organisation envisage de masquer les données sensibles en recourant à des techniques telles que le masquage des données, la pseudonymisation ou l'anonymisation.

Les techniques de pseudonymisation ou d'anonymisation peuvent masquer les données à caractère personnel, maquiller la véritable identité des personnes concernées ou toute autre information sensible, et rompre le lien entre les données à caractère personnel et l'identité de la personne concernée ou le lien entre d'autres données sensibles.

Lors du recours aux techniques de pseudonymisation ou d'anonymisation, il convient de vérifier que les données ont été correctement pseudonymisées ou anonymisées. Pour être efficace, il convient que l'anonymisation des données prenne en compte tous les éléments de l'information sensible. À titre d'exemple, si ce principe est négligé, une personne peut être identifiée même si les données qui peuvent l'identifier directement sont anonymisées, par la présence d'autres données permettant d'identifier la personne de façon indirecte.

Les autres techniques de masquage des données sont les suivantes :

a) chiffrement (exige que les utilisateurs autorisés disposent d'une clé) ;

b) annulation ou suppression de caractères (pour empêcher les utilisateurs non autorisés de visualiser les messages en entier) ;

c) changement des nombres et des dates ;

d) remplacement (remplacement d'une valeur par une autre pour masquer les données sensibles).

Il convient de considérer les éléments suivants lors de la mise en œuvre de techniques de masquage des données :

a) ne pas accorder à tous les utilisateurs l'accès à toutes les données ; concevoir des requêtes et des masques pour n'afficher que les données minimales requises à l'utilisateur ;

b) dans certains cas, il convient que des données ne soient pas visibles par l'utilisateur pour certains enregistrements parmi un ensemble de données ; dans ce cas, concevoir et mettre en œuvre un système de brouillage des données (par exemple, certains patients peuvent ne pas souhaiter que le personnel de l'hôpital ait accès à tout leur dossier, même en cas d'urgence ; dans ce cas, les utilisateurs se voient présenter des données partiellement brouillées et les données peuvent uniquement être consultées par le personnel doté des rôles spécifiques si elles contiennent des informations utiles pour permettre au patient de recevoir le traitement approprié) ;

c) lorsque des données sont brouillées, donner la possibilité à la personne concernée d'exiger que les utilisateurs ne puissent pas voir si lesdites données sont brouillées (brouillage du brouillage ; ce système est utilisé dans les établissements de santé, par exemple si le patient ne souhaite pas que le personnel voie que des données sensibles, telles que des grossesses ou des examens de sang, ont été brouillées).

Informations supplémentaires

L'anonymisation modifie les DCP de façon irréversible, de sorte que la personne concernée ne peut plus être identifiée, ni directement ni indirectement.

La pseudonymisation remplace les informations d'identification par un alias. La connaissance de l'algorithme (parfois appelé « information supplémentaire ») utilisé pour exécuter la pseudonymisation permet au moins une certaine forme d'identification de la personne concernée. Il convient donc de garder ces « informations supplémentaires » à part et de les protéger.

Bien que la pseudonymisation soit moins poussée que l'anonymisation, les ensembles de données pseudonymisés peuvent s'avérer plus utiles dans une étude statistique.

Le masquage des données peut être statique (les données sont masquées dans la base de données d'origine), dynamique (grâce à l'automatisation et à des règles permettant de sécuriser les données en temps réel) ou à la volée (les données sont masquées dans la mémoire de l'application).

Des fonctions de hachage peuvent être utilisées pour anonymiser les données à caractère personnel. Pour empêcher les attaques par énumération, il convient de toujours les associer à une fonction de salage.

Il convient d'éviter d'introduire des DCP dans les identifiants des ressources et leurs attributs (par exemple, noms de fichiers et URL) ou de les anonymiser correctement.

D'autres mesures concernant la protection des données à caractère personnel dans l'informatique en nuage public sont disponibles dans l'ISO/IEC 27018.

Des informations supplémentaires sur les techniques de dé-identification sont disponibles dans l'ISO/IEC 20889.

8.12 Prévention de la fuite de données

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Confidentialité	#Protection #Détection	#Protection_des_informations	#Protection #Défense

Mesure de sécurité

Il convient d'appliquer des mesures de prévention de la fuite de données aux systèmes, réseaux et terminaux qui traitent, stockent ou transmettent de l'information sensible.

Objectif

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

Préconisations

Il convient que l'organisation envisage les points suivants pour réduire le risque de fuite de données :

a) identifier et classifier l'information à protéger contre toute fuite (par exemple, données personnelles, modèles de tarification et conceptions de produits) ;

b) surveiller les canaux de fuite de données (par exemple, messagerie électronique, transferts de fichiers, appareils mobiles et dispositifs de stockage portables) ;

c) agir pour empêcher la fuite d'information (par exemple, mettre en quarantaine les courriers électroniques contenant de l'information sensible).

Il convient d'utiliser des outils de prévention de la fuite de données pour :

a) identifier et surveiller l'information sensible soumise à un risque de divulgation non autorisée (par exemple, dans les données non structurées du système d'un utilisateur) ;

b) détecter la divulgation d'information sensible (par exemple, lors du téléchargement d'information vers des services en nuage externes non fiables ou de l'envoi d'information par courrier électronique) ;

c) bloquer les actions utilisateur ou les transmissions réseau qui exposent de l'information sensible (par exemple, empêcher la copie d'entrées de base de données dans un tableur).

Il convient que l'organisation détermine s'il est nécessaire de limiter la possibilité pour l'utilisateur de copier et coller ou de télécharger des données vers des services, dispositifs et supports extérieurs à l'organisation. Dans l'affirmative, il convient que l'organisation mette en œuvre des outils de prévention de la fuite de données ou qu'elle configure des outils existants pour permettre aux utilisateurs d'afficher et de manipuler des données conservées à distance, mais les empêcher de les copier et coller hors du contrôle de l'organisation.

Si une exportation de données est requise, il convient que le propriétaire des données approuve l'exportation et que les utilisateurs soient tenus responsables de leurs actes.

Il convient de traiter la prise d'instantanés ou de photographies de l'écran dans les conditions d'utilisation, la formation et l'audit.

Si des données sont sauvegardées, il convient de veiller à ce que l'information sensible soit protégée par des mesures telles que le chiffrement, le contrôle d'accès et la protection des supports physiques.

Il convient également d'envisager la prévention de la fuite de données pour se protéger contre les éventuelles actions de renseignement d'un ennemi souhaitant obtenir une information confidentielle ou secrète (d'ordre géopolitique, humain, financier, commercial, scientifique ou autre) susceptible de présenter de l'intérêt à des fins d'espionnage ou pouvant s'avérer critique pour l'établissement. Il convient d'orienter les actions de prévention de la fuite de données de sorte à induire l'ennemi en erreur, par exemple en remplaçant l'information authentique par une fausse information, soit dans le cadre d'une action indépendante, soit en réponse aux actions de renseignement de l'ennemi. L'ingénierie sociale inversée ou l'utilisation de pots de miel pour attirer les attaquants constituent des exemples d'actions de ce type.

Informations supplémentaires

Les outils de prévention de la fuite de données sont destinés à identifier des données, à surveiller leur usage et leur transfert, et à entreprendre des actions visant à empêcher la fuite de données (par exemple, en alertant les utilisateurs quant à leur comportement à risque et en bloquant le transfert de données vers des dispositifs de stockage portables).

La prévention de la fuite de données implique en elle-même la surveillance des communications et activités en ligne du personnel et, par extension, des messages de tiers, ce qui soulève des considérations d'ordre légal auxquelles il convient de réfléchir avant de déployer des outils de prévention de la fuite de données. Il existe toute une série de législations en matière de confidentialité, de protection des données, d'emploi, d'interception de données et de télécommunications, applicables à la surveillance et au traitement des données dans le contexte de la prévention de la fuite de données.

La prévention de la fuite de données peut être prise en charge par des mesures de sécurité standard, telles que des politiques portant sur le thème du contrôle d'accès et la gestion des documents sécurisée (voir 5.12 et 5.15).

8.13 Sauvegarde des informations

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Correction	#Intégrité #Disponibilité	#Récupération	#Continuité	#Protection

Mesure de sécurité

Il convient de conserver des copies de sauvegarde de l'information, des logiciels et des systèmes et de les tester régulièrement à l'aide de la politique définie sur le thème de la sauvegarde.

Objectif

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

Préconisations

Il convient de définir une politique portant sur le thème de la sauvegarde pour répondre aux exigences de l'organisation en termes de conservation des données et de sécurité de l'information.

Il convient de prévoir des équipements de sauvegarde adéquats pour s'assurer que toute l'information et tous les logiciels essentiels peuvent être récupérés en cas d'incident, de défaillance d'un support ou de perte.

Il convient d'élaborer et de mettre en œuvre des plans précisant la façon dont l'organisation sauvegardera son information, ses logiciels et ses systèmes pour traiter la politique portant sur le thème de la sauvegarde.

Lors de la conception d'un plan de sauvegarde, il convient de tenir compte des éléments suivants :

a) produire des enregistrements exacts et complets des copies de sauvegarde effectuées ainsi que des procédures de restauration documentées ;

b) tenir compte des exigences métier de l'organisation (comme le point de récupération des données ; voir 5.30), des exigences de sécurité de l'information concernée et du niveau de criticité de l'information à l'égard de la continuité de l'activité pour définir l'étendue (par exemple, sauvegarde complète ou différentielle) et la fréquence des sauvegardes ;

c) stocker les sauvegardes dans un lieu sûr, suffisamment distant du site principal pour échapper à tout dommage résultant d'un sinistre sur le site principal ;

d) doter l'information sauvegardée d'un niveau de protection physique et environnementale approprié (voir l'Article 7 et 8.1), cohérent avec les normes appliquées sur le site principal ;

e) tester régulièrement les supports de sauvegarde pour s'assurer qu'il est possible de s'en servir, le cas échéant, en situation d'urgence ; tester la capacité à restaurer les données sauvegardées sur des supports de test dédiés, ne pas écraser les supports d'origine si le processus de sauvegarde ou de restauration échoue et entraîne une altération ou une perte de données irréversible ;

f) protéger les sauvegardes par le biais du chiffrement conformément aux risques identifiés (par exemple, dans des situations où la confidentialité revêt de l'importance) ;

g) veiller à s'assurer qu'une perte de données accidentelle soit détectée avant réalisation de la sauvegarde.

Il convient que les procédures d'exploitation assurent une surveillance de l'exécution des sauvegardes et remédient aux défaillances des sauvegardes programmées pour garantir l'intégralité des sauvegardes conformément à la politique portant sur le thème de la sauvegarde.

Il convient de tester régulièrement les dispositions de sauvegarde concernant les systèmes et les services individuels pour s'assurer qu'elles répondent aux objectifs des plans de réponse aux incidents et de continuité d'activité (voir 5.30). Il convient de combiner cette opération à un test des procédures de restauration et d'effectuer une vérification par rapport à la durée de restauration requise dans le plan de continuité d'activité. Pour les systèmes et les services critiques, il convient que les dispositions relatives aux sauvegardes couvrent toute l'information système, les applications et les données nécessaires à la récupération totale du système en cas de sinistre.

Si l'organisation utilise un service en nuage, il convient d'effectuer des copies de sauvegarde de l'information, des applications et des systèmes de l'organisation dans l'environnement du service en nuage. Il convient que l'organisation détermine si et comment les exigences en termes de sauvegarde sont remplies lors de l'utilisation du service de sauvegarde de l'information mis à disposition dans le cadre du service en nuage.

Il convient de déterminer la durée de conservation de l'information essentielle à l'activité de l'organisation, en prenant en compte toute exigence éventuelle de conservation de copies d'archivage. Il convient que l'organisation envisage la suppression de l'information (voir 8.10) figurant sur les supports de sauvegarde une fois que la durée de conservation de l'information concernée arrive à expiration, conformément aux exigences d'ordre légal ou réglementaire.

Informations supplémentaires

Pour de plus amples informations sur la sécurité du stockage, notamment la notion de conservation, voir l'ISO/IEC 27040.

8.14 Redondance des moyens de traitement de l'information

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Disponibilité	#Protection	#Continuité #Gestion_des_actifs	#Protection #Résilience

Mesure de sécurité

Il convient de mettre en œuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité.

Objectif

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

Préconisations

Il convient que l'organisation identifie les exigences relatives à la disponibilité des services métier et des systèmes d'information. Il convient que l'organisation conçoive et mette en œuvre une architecture de systèmes dotée de la redondance appropriée pour satisfaire à ces exigences.

La redondance peut être assurée en dupliquant les moyens de traitement de l'information en partie ou en totalité (c'est-à-dire épargner des composants ou tout doubler). Il convient que l'organisation planifie et mette en œuvre des procédures d'activation des composants et moyens de traitement redondants. Il convient que le plan établisse si les composants et activités de traitement redondants sont toujours activés, remplacés automatiquement ou activés manuellement.

Il convient de mettre en place des mécanismes visant à alerter l'organisation en cas de défaillance des moyens de traitement de l'information, à activer l'exécution de la procédure planifiée et à permettre la disponibilité continue pendant la réparation ou le remplacement des moyens de traitement de l'information.

Il convient que l'organisation prenne en compte les éléments suivants lors de la mise en œuvre de systèmes redondants :

a) conclure un contrat avec au moins deux fournisseurs de moyens de traitement de l'information critique et en réseau, tels que des fournisseurs d'accès Internet ;

b) utilisation de réseaux redondants ;

c) recours à deux centres de données séparés géographiquement, avec des systèmes en miroir ;

d) utilisation de systèmes ou de sources d'alimentation physiquement redondants ;

e) utilisation de plusieurs instances parallèles des composants logiciels, avec équilibrage de charge automatique entre eux (entre les instances d'un même centre de données ou de plusieurs centres de données) ;

f) duplication des composants dans les systèmes (par exemple, CPU, disques durs, mémoires) ou les réseaux (par exemple, pare-feu, routeurs, commutateurs).

Le cas échéant, et de préférence en mode de production, il convient de tester les systèmes d'information redondants pour s'assurer que le basculement d'un composant à un autre fonctionne comme prévu.

Informations supplémentaires

La redondance et la préparation des TIC pour la continuité d'activité sont étroitement liées (voir 5.30), notamment si des délais de rétablissement courts sont requis. La plupart des stratégies et solutions de redondance peuvent être intégrées aux stratégies et solutions de continuité liées aux TIC.

La mise en œuvre de redondances peut introduire des risques liés à l'intégrité (par exemple, les processus de copie de données sur les composants dupliqués peuvent introduire des erreurs) ou à la confidentialité (par exemple, une mesure de sécurité faible concernant les composants dupliqués peut entraîner une compromission) de l'information et des systèmes d'information, qui doivent être pris en compte lors de la conception des systèmes d'information.

En règle générale, la redondance des moyens de traitement de l'information ne résout pas l'indisponibilité des applications découlant de pannes au niveau applicatif.

Avec le recours à l'informatique en nuage public, il est possible et souhaitable de disposer de plusieurs versions opérationnelles des moyens de traitement de l'information, qui soient présentes dans plusieurs lieux physiques distincts et équipées de fonctions de basculement automatique et d'équilibrage de charge.

Des technologies et techniques de redondance et de basculement automatique dans le contexte des services en nuage sont abordées dans l'ISO/IEC TS 23167.

8.15 Journalisation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Protection #Défense

Mesure de sécurité

Il convient de créer, de protéger, de stocker et d'analyser des journaux enregistrant les activités, exceptions, pannes et autres événements pertinents.

Objectif

Enregistrer les événements, générer des preuves, garantir l'intégrité de l'information journalisée, empêcher tout accès non autorisé, identifier les événements liés à la sécurité de l'information pouvant engendrer un incident lié à la sécurité de l'information et faciliter les investigations.

Préconisations

Généralités

Il convient que l'organisation détermine les besoins pour lesquels les journaux sont créés, la nature des données collectées et journalisées et les éventuelles exigences propres aux journaux pour la protection et le traitement des données qui y sont consignées. Il convient de documenter ces aspects dans un plan de collecte et de journalisation.

Il convient que les journaux d'événements contiennent les renseignements suivants pour chaque événement :

a) les identifiants utilisateurs ;

b) les activités du système ;

c) la date, l'heure et les détails relatifs aux événements pertinents, par exemple les ouvertures et fermetures de session ;

d) l'identité du dispositif, l'identifiant système et son emplacement ;

e) les adresses et protocoles réseau.

Il convient de prendre en compte les événements suivants dans le cadre de la journalisation :

a) les tentatives d'accès au système réussies et avortées ;

b) les tentatives d'accès aux données et autres ressources, réussies et avortées ;

c) les modifications apportées à la configuration du système ;

d) l'utilisation de privilèges ;

e) l'utilisation de programmes utilitaires et d'applications ;

f) les fichiers consultés et le type d'accès, y compris la suppression de fichiers de données importants ;

g) les alarmes déclenchées par le système de contrôle d'accès ;

h) l'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection d'intrusion ;

i) la création, modification ou suppression d'identités ;

j) les transactions exécutées par les utilisateurs dans les applications. Dans certains cas, les applications correspondent à un service ou produit fourni ou exécuté par une tierce partie.

La journalisation des événements pose les fondations des systèmes de surveillance automatisés (voir 8.16), capables de générer des rapports consolidés et des alertes relatives à la sécurité du système.

Elle est importante pour tous les systèmes qui ont des sources d'heure synchronisées (voir 8.17) dans la mesure où elle permet la corrélation des journaux entre les systèmes dans l'éventualité d'une investigation liée à un incident.

Protection des journaux

Il convient que les utilisateurs, y compris ceux dotés de privilèges d'accès, n'aient pas l'autorisation de supprimer ni de désactiver les journaux relatifs à leurs propres activités. Ils peuvent être à même de manipuler les journaux sur les moyens de traitement de l'information qu'ils contrôlent directement : il est donc nécessaire de protéger et de revoir les journaux afin de garantir l'imputabilité des utilisateurs dotés de privilèges.

Il convient que des mesures soient conçues pour protéger le moyen de journalisation contre les modifications non autorisées de la journalisation des informations et les dysfonctionnements, à savoir :

a) l'altération des types de message enregistrés ;

b) la modification ou la suppression des fichiers journaux ;

c) le dépassement de la capacité du support de stockage du fichier journal, qui a pour effet d'empêcher l'enregistrement des événements ou d'écraser les événements déjà enregistrés.

Pour la protection des journaux, il convient d'envisager de recourir aux techniques suivantes : hachage cryptographique, enregistrement dans un fichier en ajout seulement et en lecture seule, enregistrement dans un fichier de transparence public.

Il peut être nécessaire d'archiver certains journaux d'audit en raison d'exigences liées à la conservation des données ou au recueil et à la conservation de preuves (voir 5.28).

Si l'organisation doit envoyer des journaux système ou d'application à un fournisseur pour l'aider à résoudre des erreurs de débogage ou de dépannage, il convient de désidentifier les journaux, si possible à l'aide de techniques de masquage des données (voir 8.11) ciblant les informations telles que les noms d'utilisateurs, les adresses IP, les noms d'hôtes et le nom de l'organisation, avant l'envoi au fournisseur.

Les journaux d'événements peuvent contenir des données sensibles et des données à caractère personnel. Il convient de prendre les mesures de protection de la vie privée (voir 5.34) appropriées.

Analyse des journaux

Il convient que l'analyse des journaux englobe l'analyse et l'interprétation des événements liés à la sécurité de l'information pour faciliter l'identification de tout comportement anormal ou activité inhabituelle, pouvant représenter un signe de compromission.

Il convient de tenir compte des éléments suivants lors de l'analyse des événements :

a) les compétences dont doivent disposer les experts qui procèdent à l'analyse ;

b) la détermination de la procédure d'analyse des journaux ;

c) les attributs exigés de chaque événement lié à la sécurité ;

d) les exceptions identifiées grâce à l'utilisation des règles prédéfinies (par exemple, SIEM ou règles de pare-feu et IDS ou signatures de programmes malveillants) ;

e) les modèles de comportement connus et le trafic réseau standard comparés à un comportement et une activité anormaux (analyse comportementale des utilisateurs et des entités [user and entity behaviour analytics ou UEBA]) ;

f) les résultats de l'analyse des tendances ou des modèles (par exemple, consécutivement à l'utilisation d'analyses de données, de techniques de big data et d'outils d'analyse spécialisés) ;

g) l'intelligence des menaces disponible.

Il convient d'appuyer l'analyse des journaux par des activités de surveillance spécifiques facilitant l'identification et l'analyse des comportements anormaux, notamment :

a) le passage en revue des tentatives d'accès aux ressources protégées (par exemple, serveurs DNS, portails Internet et partages de fichiers), réussies ou avortées ;

b) la consultation des journaux DNS pour identifier les connexions réseau sortantes à des serveurs malveillants, tels que ceux associés à la commande et au contrôle de botnets ;

c) l'examen des rapports d'utilisation émis par les fournisseurs de services (par exemple, factures ou rapports de service) en cas d'activité inhabituelle au niveau des systèmes ou des réseaux (par exemple, en étudiant des modèles d'activité) ;

d) la prise en compte des journaux d'événements de surveillance physique, dont les entrées et les sorties, pour assurer une détection et une analyse des incidents plus précises ;

e) la corrélation des journaux en vue d'analyses efficaces et d'une extrême précision.

Il convient d'identifier les incidents liés à la sécurité de l'information avérés et suspectés (tels qu'une infection par un programme malveillant ou le sondage des pare-feu) et de les soumettre à des investigations plus poussées (par exemple dans le cadre d'un processus de management de la sécurité de l'information ; voir 5.25).

Informations supplémentaires

Les journaux système contiennent souvent un volume d'information important. La plus grande partie de cette information ne concerne pas la surveillance liée à la sécurité de l'information. Pour faciliter l'identification des événements importants dans le cadre de la surveillance de la sécurité de l'information, on peut envisager de recourir à des programmes utilitaires ou des outils d'audit adaptés permettant de procéder à une interrogation des fichiers.

Un outil de gestion de l'information et des événements de sécurité (ou outil SIEM pour Security information and event management) ou un service équivalent peut être utilisé pour stocker, corréler, normaliser et analyser les informations des journaux ainsi que pour générer des alertes. Les outils SIEM tendent à exiger certaines précautions en matière de configuration pour procurer des avantages optimaux. Les configurations à envisager comprennent l'identification et la sélection des sources des journaux, le réglage et le test des règles, et le développement de cas d'utilisation.

Les fichiers de transparence publics pour l'enregistrement des journaux sont, par exemple, utilisés dans les systèmes de transparence des certificats. Les fichiers de ce type peuvent procurer un mécanisme de détection additionnel permettant de protéger l'organisation contre la falsification des journaux.

8.16 Activités de surveillance

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Mesure de sécurité

Il convient de surveiller les réseaux, systèmes et applications pour détecter tout comportement anormal et de prendre les mesures appropriées pour évaluer les incidents liés à la sécurité de l'information potentiels.

Objectif

Détecter les comportements anormaux et les incidents liés à la sécurité de l'information potentiels.

Préconisations

Il convient de déterminer l'étendue et le niveau de la surveillance conformément aux exigences métier et de sécurité de l'information ainsi qu'aux lois et réglementations applicables en la matière. Il convient de conserver les enregistrements de surveillance pendant les durées de conservation définies.

Il convient de prendre en compte les éléments suivants concernant l'intégration au système de surveillance :

a) trafic entrant et sortant au niveau des réseaux, systèmes et applications ;

b) accès aux systèmes, aux serveurs, à l'équipement réseau, au système de surveillance, aux applications critiques, etc. ;

c) fichiers de configuration système et réseau de nature critique ou d'administration ;

d) journaux générés par les outils de sécurité (par exemple, antivirus, IDS, IPS, filtres Web, pare-feu, prévention de la fuite de données) ;

e) journaux d'événements en lien avec l'activité système ou réseau ;

f) vérification du code en cours d'exécution pour déterminer s'il est autorisé dans le système et s'il n'a pas subi d'altération (par exemple, via une recompilation visant à y ajouter du code indésirable) ;

g) utilisation des ressources (par exemple, CPU, disques durs, mémoire vive, bande passante) et performances correspondantes.

Il convient que l'organisation établisse une base de référence du comportement considéré comme normal et qu'elle exécute la surveillance des anomalies par rapport à cette base. Lors de l'établissement d'une base de référence, il convient de tenir compte des éléments suivants :

a) examen de l'utilisation des systèmes pendant les périodes normales et les périodes de pic ;

b) habitude de chaque utilisateur ou groupe d'utilisateurs concernant l'heure d'accès, le lieu d'accès et la fréquence d'accès.

Il convient de configurer le système de surveillance par rapport à la base de référence établie pour identifier tout comportement anormal, tel que :

a) interruption non planifiée de processus ou d'applications ;

b) activité généralement associée à des programmes malveillants ou trafic en provenance d'adresses IP ou de domaines réseau malveillants connus (comme ceux associés à des serveurs de commande et de contrôle de botnets) ;

c) caractéristiques d'attaque connues (par exemple, déni de service et débordements de mémoire tampon) ;

d) comportement inhabituel du système (par exemple, enregistrement de frappe, injection de processus et divergences dans l'utilisation des protocoles standard) ;

e) goulots d'étranglement et surcharges (par exemple, mise en file d'attente sur le réseau, niveaux de latence et gigue réseau) ;

f) accès non autorisé (y compris tentative) aux systèmes ou à l'information ;

g) analyse non autorisée d'applications métier, de systèmes et de réseaux ;

h) tentatives d'accès aux ressources protégées (par exemple, serveurs DNS, portails Internet et systèmes de fichiers), réussies ou avortées ;

i) comportement inhabituel d'un utilisateur et d'un système par rapport au comportement attendu.

Il convient de mettre en place une surveillance continue via un outil de surveillance. Il convient d'effectuer la surveillance en temps réel ou à intervalles réguliers, sous réserve des besoins et capacités de l'organisation. Il convient que les outils de surveillance offrent la possibilité de gérer d'importants volumes de données, de s'adapter à la constante évolution des menaces et qu'ils prévoient la notification en temps réel. Il convient également que les outils puissent reconnaître certaines signatures et des modèles de comportement pour les données, réseaux ou applications.

Il convient de configurer le logiciel de surveillance automatisée en vue de la génération d'alertes (par exemple, via une console de gestion, des messages électroniques ou des SMS adressés à des téléphones portables) sur la base de seuils prédéfinis. Il convient également de régler le système d'alerte et de le soumettre à un apprentissage de la base de référence de l'organisation afin de réduire au minimum les faux positifs. Il convient d'affecter du personnel à la réponse aux alertes et de le former correctement à l'interprétation précise des incidents potentiels. Il convient de mettre en place des systèmes et processus redondants pour recevoir les notifications d'alerte et y répondre.

Il convient de communiquer les événements anormaux aux parties concernées afin d'améliorer les activités suivantes : audit, évaluation de la sécurité, analyse des vulnérabilités et surveillance (voir 5.25). Il convient de mettre en place des procédures pour répondre aux indicateurs positifs du système de surveillance dans les meilleurs délais et réduire au minimum les conséquences des événements indésirables sur la sécurité (voir 5.26). Il convient également de définir des procédures pour identifier et traiter les faux positifs, notamment le réglage du logiciel de surveillance pour réduire le nombre de futurs faux positifs.

Informations supplémentaires

La surveillance de la sécurité peut être améliorée par les biais suivants :

a) exploitation de systèmes d'intelligence des menaces (voir 5.7) ;

b) exploitation de l'apprentissage automatique et des capacités de l'intelligence artificielle ;

c) listes de blocage ou listes d'autorisation ;

d) réalisation de différentes évaluations de la sécurité technique (par exemple, évaluations des vulnérabilités, tests de pénétration, simulations de cyberattaques et exercices de réponse aux cyberattaques) ; et utilisation de ces évaluations pour déterminer les bases de référence ou les comportements acceptables ;

e) utilisation de systèmes de contrôle des performances pour faciliter la définition et la détection des comportements anormaux ;

f) exploitation des journaux conjointement avec les systèmes de surveillance.

Les activités de surveillance sont souvent menées à l'aide de logiciels spécialisés, tels que les systèmes de détection d'intrusion. Ces derniers peuvent être configurés par rapport à une base de référence des activités système et réseau considérées comme normales, acceptables et attendues.

La surveillance visant à identifier les communications anormales facilite l'identification des botnets (ensemble de dispositifs sous le contrôle malveillant du propriétaire des botnets, habituellement utilisé pour lancer des attaques par déni de service distribué sur les ordinateurs d'autres organisations). Si l'ordinateur est contrôlé par un dispositif externe, une communication est établie entre le dispositif contrôlé et celui qui le contrôle. Il convient donc que l'organisation emploie des technologies permettant d'identifier les communications anormales et de prendre les mesures nécessaires.

8.17 Synchronisation des horloges

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Détection	#Intégrité	#Protection #Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Protection #Défense

Mesure de sécurité

Il convient que les horloges des systèmes de traitement de l'information utilisés par l'organisation soient synchronisées avec les sources de temps approuvées.

Objectif

Permettre la corrélation et l'analyse des événements liés à la sécurité et des autres données enregistrées, et la prise en charge des investigations ayant trait aux incidents liés à la sécurité de l'information.

Préconisations

Il convient de documenter et de mettre en œuvre les exigences internes et externes liées à la représentation de l'heure, la fiabilité de la synchronisation et la précision. Ces exigences peuvent correspondre à des exigences légales, statutaires, réglementaires ou contractuelles, des exigences de conformité à des normes et aux besoins de surveillance interne. Il convient de définir et de prendre en compte une heure de référence standard à utiliser dans l'organisation pour tous les systèmes, y compris les systèmes de gestion du bâtiment, les systèmes d'entrée et de sortie et autres, qui peuvent être utilisés pour faciliter les investigations.

Pour les systèmes de journalisation, il convient d'utiliser une horloge de référence reliée à un signal horaire radiodiffusé par une horloge atomique nationale ou un GPS ; une source de date et heure cohérente, de confiance, pour garantir l'exactitude des horodatages. Il convient d'utiliser un protocole NTP pour garantir la synchronisation de tous les systèmes avec l'horloge de référence. Pour améliorer la fiabilité des horloges externes, il convient que l'organisation utilise deux sources d'heure externes en même temps et gère les écarts éventuels de manière appropriée.

La synchronisation des horloges peut s'avérer difficile si l'organisation utilise plusieurs services en nuage ou si elle utilise conjointement des services en nuage et des solutions sur site. Dans ce cas, il convient de gérer l'horloge de chaque service et l'écart enregistré.

Informations supplémentaires

Le paramétrage correct des horloges est important pour garantir la précision des journaux d'événements qui peuvent être utilisés lors d'investigations ou servir de preuves dans le cadre d'affaires judiciaires ou de procédures disciplinaires. Des journaux d'audit imprécis peuvent gêner les investigations et nuire à la crédibilité des preuves.

8.18 Utilisation de programmes utilitaires à privilèges

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau #Configuration_sécurisée	#Protection

Mesure de sécurité

Il convient de limiter et de contrôler étroitement l'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application.

Objectif

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

Préconisations

Il convient de prendre en compte les lignes directrices suivantes en matière d'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application :

a) limiter l'emploi des programmes utilitaires à un nombre minimal acceptable d'utilisateurs de confiance bénéficiant d'une autorisation (voir 8.2) ;

b) utiliser des procédures d'identification, d'authentification et d'autorisation pour les programmes utilitaires, y compris l'identification unique de la personne qui utilise le programme utilitaire ;

c) définir et documenter les niveaux d'autorisation relatifs aux programmes utilitaires ;

d) autoriser une utilisation ad hoc des programmes utilitaires ;

e) ne pas mettre de programmes utilitaires à la disposition des utilisateurs ayant accès à des applications dépendant de systèmes dans lesquels la séparation des tâches est requise ;

f) désinstaller ou désactiver tous les programmes utilitaires inutiles ;

g) au minimum, séparer de façon logique les programmes utilitaires des logiciels d'application. Dans la mesure du possible, séparer les communications réseau liées à ces programmes du trafic des applications ;

h) poser des limites à la disponibilité des programmes utilitaires, par exemple limiter la durée d'une autorisation de modification ;

i) journaliser toutes les utilisations de programmes utilitaires.

Informations supplémentaires

La plupart des systèmes d'information sont dotés d'un ou plusieurs programmes utilitaires qui peuvent avoir la capacité de contourner les mesures de sécurité d'un système ou d'une application, par exemple les diagnostics, l'application de correctifs, les antivirus, les outils de défragmentation de disque, les débogueurs, les outils de sauvegarde et les outils réseau.

8.19 Installation de logiciels sur des systèmes en exploitation

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Configuration_sécurisée	#Protection

Mesure de sécurité

Il convient de mettre en œuvre des procédures et des mesures permettant une gestion sécurisée de l'installation de logiciels dans les systèmes opérationnels.

Objectif

Assurer l'intégrité des systèmes opérationnels et empêcher l'exploitation des vulnérabilités techniques.

Préconisations

Pour gérer de façon sécurisée les changements et installations de logiciels dans les systèmes opérationnels, il convient de prendre en compte les lignes directrices suivantes :

a) réserver l'installation des mises à jour de logiciels opérationnels à des administrateurs qualifiés, après autorisation de la direction (voir 8.5) ;

b) s'assurer que seul du code exécutable approuvé et non du code de développement ou des compilateurs soit installé dans les systèmes opérationnels ;

c) n'installer et ne mettre à jour un logiciel qu'au terme d'une série complète de tests ayant donné des résultats satisfaisants (voir 8.29 et 8.31) ;

d) mettre à jour toutes les bibliothèques de programmes sources correspondantes ;

e) utiliser un système de contrôle de la configuration afin de conserver le contrôle de tous les logiciels opérationnels, ainsi que de la documentation système ;

f) définir une stratégie de retour en arrière avant d'appliquer des modifications ;

g) tenir un journal d'audit de toutes les mises à jour des logiciels opérationnels ;

h) conserver les versions précédentes du logiciel à titre de mesure de secours ;

i) archiver les versions précédentes du logiciel, ainsi que toute l'information nécessaire, les paramètres, les procédures, les détails de configuration et les logiciels complémentaires associés, aussi longtemps que le logiciel doit lire ou traiter les données archivées.

Il convient que toute décision d'acquérir une nouvelle version tienne compte des exigences métier à l'origine du changement, ainsi que des questions de sécurité liées à la nouvelle version, à savoir l'introduction d'une nouvelle fonction de sécurité de l'information ou le nombre et la gravité des vulnérabilités en termes de sécurité de l'information liées à la version actuelle. Il convient d'appliquer des correctifs logiciels chaque fois qu'ils permettent de supprimer ou de réduire les vulnérabilités en termes de sécurité de l'information (voir 8.8, 8.19).

Les logiciels peuvent dépendre de logiciels et de packages fournis par un tiers (par exemple, programmes de logiciels utilisant des modules hébergés sur des sites externes) qu'il convient de surveiller et de contrôler afin d'éviter tout changement non autorisé susceptible d'introduire des vulnérabilités en termes de sécurité de l'information.

Pour les logiciels fournis par l'éditeur et installés dans les systèmes opérationnels, il convient d'assurer une maintenance permettant de bénéficier de l'assistance technique de l'éditeur. Au fil du temps, les éditeurs de logiciels cessent de fournir une assistance technique pour les anciennes versions. Il convient que l'organisation tienne compte des risques associés à l'utilisation de logiciels dont la maintenance n'est pas prise en charge par l'éditeur. Il convient que les logiciels libres (« open source ») utilisés dans les systèmes opérationnels fassent l'objet d'une maintenance jusqu'à la toute dernière version du logiciel. Au fil du temps, la maintenance du code open source peut s'arrêter, mais celui-ci reste disponible dans un référentiel de logiciels libres. Il convient également que l'organisation considère les risques liés à l'utilisation de logiciels libres sans maintenance dans le cadre des systèmes opérationnels.

Lorsque l'éditeur participe à l'installation ou à la mise à jour du logiciel, il convient de n'accorder l'accès physique ou logique qu'en cas de nécessité et avec l'autorisation appropriée. Il convient de surveiller les activités de l'éditeur (voir 5.22).

Il convient que l'organisation détermine et impose des règles strictes quant aux types de logiciels que les utilisateurs peuvent installer.

Il convient d'appliquer le principe du moindre privilège à l'installation de logiciels dans les systèmes opérationnels. Il convient que l'organisation détermine les types de logiciels dont l'installation est autorisée (par exemple l'installation des mises à jour ou de correctifs à des logiciels existants) et les types d'installation qui sont interdits (par exemple, l'installation de logiciels destinés uniquement à un usage personnel, ou de logiciels dont on ignore s'ils sont potentiellement malveillants ou pour lesquels on éprouve des doutes). Il convient d'accorder ces privilèges en tenant compte des fonctions des utilisateurs concernés.

Informations supplémentaires

L'installation non contrôlée de logiciels sur des dispositifs informatiques peut entraîner l'introduction de vulnérabilités. Les vulnérabilités peuvent entraîner des incidents liés à la sécurité de l'information, tels que le vol d'identité, la fuite d'information, la perte d'intégrité ou la violation des droits de propriété intellectuelle. Lorsque le code source de l'éditeur est injecté de façon dynamique, par exemple dans des applications SaaS, il peut s'avérer difficile de valider un logiciel de ce type. L'utilisation d'un tel logiciel uniquement par des personnes de confiance peut réduire les points faibles en termes de sécurité.

8.20 Mesures liées aux réseaux

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection

Mesure de sécurité

Il convient de gérer et de contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications.

Objectif

Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

Préconisations

Il convient de mettre en œuvre des mesures pour assurer la sécurité de l'information sur les réseaux et protéger les services connectés contre tout accès non autorisé. Il convient d'envisager en particulier ce qui suit :

a) le type et le niveau de classification de l'information que le réseau peut prendre en charge ;

b) définir les responsabilités et les procédures de gestion de l'équipement réseau et des dispositifs correspondants ;

c) tenir la documentation à jour, notamment les schémas de réseau et les fichiers de configuration des dispositifs, tels que les routeurs et les commutateurs ;

d) séparer la responsabilité opérationnelle des réseaux et des opérations des systèmes de TIC, le cas échéant (voir 5.3) ;

e) définir des mesures pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics, les réseaux tiers ou les réseaux sans fil et protéger les systèmes et applications connectés (voir 5.22, 8.24, 5.14 et 6.6). Des mesures spéciales peuvent aussi s'avérer nécessaires pour maintenir la disponibilité des services en réseau et des ordinateurs connectés au réseau ;

f) procéder à une journalisation et assurer la surveillance appropriées pour permettre l'enregistrement et la détection d'actions susceptibles d'affecter la sécurité de l'information ou qui s'avèrent pertinentes pour la sécurité de l'information (voir 8.16 et 8.15) ;

g) coordonner étroitement les activités de gestion de réseau à la fois pour optimiser le service fourni à l'organisation et pour s'assurer que les mesures sont appliquées de façon homogène à travers toute l'infrastructure de traitement de l'information ;

h) authentifier les systèmes sur le réseau ;

i) restreindre et filtrer la connexion des systèmes au réseau (par exemple, à l'aide de pare-feu) ;

j) détecter, restreindre et authentifier la connexion d'équipements et de dispositifs au réseau ;

k) renforcer la sécurité des dispositifs réseau ;

l) séparer les canaux d'administration réseau de tout autre trafic réseau ;

m) isoler temporairement les sous-réseaux critiques (par exemple, avec des ponts-levis) si le réseau est attaqué.

Il convient que l'organisation veille à appliquer les mesures de sécurité appropriées à l'utilisation de réseaux virtuels. La virtualisation des réseaux englobe également les réseaux définis par logiciel (SDN, SD-WAN). Les réseaux virtuels peuvent s'avérer intéressants du point de vue de la sécurité ; ils permettent, en effet, la séparation logique des communications qui interviennent sur les réseaux physiques, en particulier pour les systèmes et applications mis en œuvre par le biais de l'informatique distribuée.

Informations supplémentaires

De plus amples informations sur la sécurité réseau sont disponibles dans l'ISO/IEC 27033 (toutes les parties).

Des informations complémentaires sur les réseaux virtuels sont disponibles dans l'ISO/IEC TS 23167.

8.21 Sécurité des services en réseau

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection

Mesure de sécurité

Il convient d'identifier, de mettre en œuvre et de surveiller les mécanismes de sécurité, les niveaux de service et les exigences de services des services en réseau.

Objectif

Garantir la sécurité dans le cadre de l'utilisation des services en réseau.

Préconisations

Il convient d'identifier et de mettre en œuvre les dispositions de sécurité nécessaires à des services en particulier, telles que les fonctions de sécurité, les niveaux de service et les exigences de services, en faisant intervenir des fournisseurs de services en réseau internes ou externes. Il convient que l'organisation s'assure que les fournisseurs de services en réseau mettent ces mesures en œuvre.

Il convient de déterminer et de surveiller régulièrement la capacité du fournisseur de services en réseau à gérer ses services de façon sécurisée. Il convient également que l'organisation et le fournisseur concluent un accord sur le droit à auditer. En outre, il convient que l'organisation prenne en compte les attestations de tiers délivrées par les fournisseurs de services pour prouver qu'ils appliquent les mesures de sécurité appropriées.

Il convient de définir des règles relatives à l'utilisation des réseaux et des services en réseau, couvrant les aspects suivants :

a) les réseaux et les services en réseau auxquels l'accès a été accordé ;

b) les exigences d'authentification pour l'accès aux différents services en réseau ;

c) les procédures d'autorisation désignant les personnes autorisées à accéder à tel ou tel réseau et service en réseau ;

d) les procédures et mesures technologiques et de gestion de réseau destinées à protéger l'accès aux connexions réseau et aux services en réseau ;

e) les moyens utilisés pour accéder aux réseaux et aux services en réseau (par exemple, réseau privé virtuel ou réseau sans fil) ;

f) l'heure, le lieu et les autres attributs de l'utilisateur au moment de l'accès ;

g) la surveillance de l'utilisation des services en réseau.

Informations supplémentaires

Les services en réseau comprennent la fourniture de connexions, les services de réseau privé et les solutions de management de la sécurité réseau, comme les pare-feu et les systèmes de détection d'intrusion. Ces services peuvent aller du simple octroi d'une bande passante non gérée à des offres à valeur ajoutée complexes.

Les fonctions de sécurité des services en réseau peuvent consister en :

a) une technologie s'appliquant à la sécurité des services en réseau, comme l'authentification, le chiffrement et les contrôles de connexion au réseau ;

b) l'exigence de paramètres techniques pour une connexion sécurisée aux services en réseau, conformément aux règles sur la sécurité et la connexion au réseau ;

c) la mise en cache, par exemple dans un réseau de livraison de contenu, et ses paramètres qui permettent aux utilisateurs de choisir l'utilisation de la mise en cache conformément aux exigences de confidentialité, de disponibilité et de performances ;

d) des procédures d'utilisation des services en réseau pour restreindre, le cas échéant, l'accès aux services ou aux applications réseau.

Des recommandations supplémentaires concernant la gestion des accès sont disponibles dans l'ISO/IEC 29146.

8.22 Filtrage Internet

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection

Mesure de sécurité

Il convient de gérer l'accès aux sites Web externes pour réduire l'exposition à tout contenu malveillant.

Objectif

Protéger les systèmes de la compromission par des programmes malveillants et empêcher l'accès aux ressources Internet non autorisées.

Préconisations

Il convient que l'organisation réduise les risques que son personnel accède à des sites Web contenant de l'information illégale ou connus pour contenir des virus ou du matériel de hameçonnage. Pour cela, une technique consiste à bloquer l'adresse IP ou le domaine du ou des sites Web concernés. Certains navigateurs et certaines technologies de protection contre les programmes malveillants exécutent cette opération automatiquement ou peuvent être configurés dans cette optique.

Il convient que l'organisation identifie les types de sites Web auxquels le personnel doit avoir accès ou non. Il convient que l'organisation envisage de bloquer l'accès aux sites Web suivants :

a) sites Web comportant une fonction de téléchargement d'information, sauf si cela est autorisé pour des raisons professionnelles valables ;

b) sites Web connus pour leur caractère malveillant ou suspectés de l'être, comme ceux qui diffusent des programmes malveillants ou du contenu de hameçonnage ;

c) serveurs de commande et de contrôle ;

d) site Web malveillant acquis via l'intelligence des menaces (voir 5.7) ;

e) sites Web partageant du contenu illégal.

Avant de déployer cette mesure de sécurité, il convient que l'organisation définisse des règles relatives à l'utilisation sûre des ressources en ligne, en précisant les restrictions éventuelles d'accès aux sites et applications Web indésirables ou inappropriés. Il convient de tenir les règles à jour.

Il convient de former le personnel à l'utilisation sûre et appropriée des ressources en ligne, ce qui comprend l'accès au Web. Il convient que la formation inclue les règles de l'organisation, le point de contact pour aborder les problèmes liés à la sécurité et le processus d'exception auquel recourir lorsque le personnel a besoin d'accéder à des ressources Internet soumises à restriction, pour des raisons professionnelles légitimes. Lors de la formation, il convient également d'apprendre au personnel qu'il doit veiller à n'outrepasser aucun avis de sécurité du navigateur signalant qu'un site Web n'est pas sûr, tout en permettant à l'utilisateur de continuer.

Informations supplémentaires

Le filtrage Internet peut comprendre différentes techniques, telles que des signatures, l'heuristique, la liste des sites Web ou domaines acceptables, la liste des sites Web ou domaines interdits et la configuration sur mesure pour contribuer à empêcher les logiciels malveillants et toute autre activité nuisible d'attaquer le réseau et les systèmes de l'organisation.

8.23 Cloisonnement des réseaux

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection

Mesure de sécurité

Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés dans les réseaux de l'organisation.

Objectif

Diviser le réseau en définissant des limites de sécurité pour contrôler le trafic qui intervient entre ces limites en fonction des besoins liés à l'activité.

Préconisations

Il convient que l'organisation envisage de gérer la sécurité des réseaux de grande envergure en les divisant en domaines réseau distincts et en les séparant du réseau public (Internet). Les domaines peuvent être choisis à partir des niveaux de confiance, de criticité et de sensibilité (par exemple domaine d'accès public, domaine poste de travail, domaine serveur, systèmes à fort et faible impact), par service administratif (par exemple ressources humaines, financier, marketing) ou par combinaison (par exemple, connexion du domaine serveur à plusieurs services administratifs). Le cloisonnement peut être réalisé en utilisant des réseaux physiques différents ou des réseaux logiques différents.

Il convient de bien définir le périmètre de chaque domaine. Si l'accès entre les différents domaines réseau est autorisé, il convient de le contrôler au niveau du périmètre en utilisant une passerelle (par exemple, pare-feu, routeur-filtre). Il convient de déterminer les critères de cloisonnement des réseaux en domaines et l'accès autorisé au-delà des passerelles en s'appuyant sur une appréciation des exigences de sécurité propres à chaque domaine. Il convient que cette appréciation soit en conformité avec la politique portant sur le thème du contrôle d'accès (voir 5.15), les exigences d'accès, la valeur et la classification de l'information traitée et qu'elle prenne également en compte le coût relatif et les répercussions sur les performances de l'incorporation d'une technologie de passerelle appropriée.

À noter que les réseaux sans fil nécessitent un traitement spécial en raison d'une mauvaise définition du périmètre du réseau. Il convient d'envisager un ajustement de la couverture radio pour le cloisonnement des réseaux sans fil. Dans le cas des environnements sensibles, il convient de veiller à traiter l'ensemble des accès sans fil comme des connexions externes et de séparer ces accès des réseaux internes jusqu'au franchissement de la passerelle conformément aux mesures de sécurité liées aux réseaux (voir 8.20), avant d'accorder l'accès aux systèmes internes. Il convient de séparer le réseau d'accès sans fil destiné aux invités des réseaux utilisés par le personnel si celui-ci utilise uniquement des terminaux utilisateurs contrôlés en conformité avec les politiques portant sur des thèmes de l'organisation.

Informations supplémentaires

Les réseaux s'étendent souvent au-delà des limites des organisations, au gré des partenariats commerciaux qui nécessitent l'interconnexion ou le partage des moyens de traitement de l'information et des moyens de réseautique. Ce type d'extension est susceptible d'augmenter le risque d'accès non autorisé aux systèmes d'information de l'organisation connectés au réseau : il s'avère nécessaire de protéger certains systèmes particulièrement sensibles ou critiques des autres utilisateurs du réseau.

8.24 Utilisation de la cryptographie

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité	#Protection	#Configuration_sécurisée	#Protection

Mesure de sécurité

Il convient de définir et de mettre en œuvre des règles relatives à l'utilisation de la cryptographie, notamment la gestion des clés cryptographiques.

Objectif

Garantir une utilisation correcte et efficace de la cryptographie pour protéger la confidentialité, l'authenticité ou l'intégrité de l'information en conformité avec les exigences légales, statutaires, réglementaires ou contractuelles en matière de cryptographie.

Préconisations

Généralités

En matière de cryptographie, il convient de prendre en compte les éléments suivants :

a) l'approche de la direction en ce qui concerne l'utilisation de la cryptographie au sein de l'organisation, y compris les principes généraux de protection de l'information ;

b) l'identification du niveau de protection nécessaire et la classification de l'information, éléments nécessaires pour définir le type, la force et la qualité de l'algorithme cryptographique requis ;

c) l'utilisation de la cryptographie pour protéger l'information stockée sur terminal final mobile ou support amovible et transmise à des dispositifs du même type via les réseaux ;

d) l'approche de gestion des clés, notamment les méthodes à utiliser pour protéger les clés cryptographiques et récupérer des informations chiffrées en cas de perte, de compromission ou d'endommagement des clés ;

e) les rôles et responsabilités concernant :

   1) la mise en œuvre des règles en vue d'une utilisation efficace de la cryptographie ;

   2) la gestion des clés, notamment leur génération (voir 8.24) ;

f) les normes à adopter ainsi que les algorithmes cryptographiques, le niveau du chiffrement et les pratiques d'utilisation pour une mise en œuvre efficace dans l'ensemble de l'organisation (quelle solution pour quel processus métier ?) ;

g) l'incidence du chiffrement de l'information dans le cas des mesures reposant sur l'analyse de contenu (par exemple, la détection de programmes malveillants ou le filtrage de contenu).

Lors de la mise en œuvre des règles de l'organisation pour une utilisation efficace de la cryptographie, il convient de tenir compte de la réglementation et des restrictions nationales pouvant s'appliquer aux techniques cryptographiques dans différentes régions du monde, ainsi que des questions de circulation transfrontalière de l'information chiffrée (voir 5.31).

Il convient que l'organisation crée une liste des solutions de cryptographie qui sont approuvées ou que le personnel a l'obligation d'utiliser dans l'organisation.

Il convient que les accords de service ou les contrats conclus avec des fournisseurs externes de services cryptographiques, par exemple une autorité de certification, couvrent les questions de responsabilité juridique, de fiabilité des services et de réactivité dans la fourniture de ces services (voir 5.22).

Gestion des clés

Une gestion appropriée des clés exige des processus sécurisés de génération, de stockage, d'archivage, d'extraction, d'attribution, de retrait et de destruction des clés cryptographiques.

Il convient que le système de gestion des clés repose sur une série convenue de normes, de procédures et de méthodes sécurisées en vue de :

a) générer des clés pour divers systèmes cryptographiques et diverses applications ;

b) générer et obtenir des certificats de clés publiques ;

c) attribuer des clés aux entités prévues et leur indiquer la procédure d'activation à la réception des clés ;

d) stocker les clés, et notamment définir comment les utilisateurs autorisés peuvent accéder aux clés ;

e) mettre à jour ou remplacer les clés, en prévoyant des règles portant sur les moments auxquels changer les clés et la façon de procéder ;

f) traiter les clés compromises ;

g) révoquer les clés, notamment le mode de retrait ou de désactivation des clés, par exemple lorsque les clés sont compromises ou lorsqu'un utilisateur quitte l'organisation (auquel cas il convient également d'archiver les clés) ;

h) récupérer les clés perdues ou altérées ;

i) sauvegarder ou archiver les clés ;

j) détruire les clés ;

k) journaliser et auditer les activités liées à la gestion des clés ;

l) fixer des dates d'activation et de désactivation, de sorte que les clés ne puissent être utilisées que pendant la période de temps définie dans les règles de gestion des clés correspondantes ;

m) répondre aux exigences légales d'accès aux clés cryptographiques ; par exemple, il peut être nécessaire de décrypter de l'information utilisée comme preuve dans le cadre d'un procès.

Il convient de protéger toutes les clés cryptographiques contre tout risque de modification ou de perte. En outre, il est nécessaire de protéger les clés secrètes et privées contre toute utilisation, ainsi que contre toute divulgation non autorisées. Il convient de prévoir une protection physique du matériel utilisé pour générer, stocker et archiver les clés, si besoin.

Outre l'intégrité, il convient, dans de nombreux cas d'utilisation, de tenir compte de l'authenticité des clés publiques.

Informations supplémentaires

L'authenticité des clés publiques est généralement prise en charge par des processus de gestion des clés publiques, par le biais d'autorités de certification et de certificats de clé publique, mais il est également possible de la prendre en charge en ayant recours à des technologies du type blockchain ou, pour un nombre de clés réduit, en appliquant des processus manuels.

La cryptographie peut être utilisée pour répondre à différents objectifs de sécurité de l'information tels que :

a) la confidentialité : le chiffrement des données permet de protéger l'information sensible ou critique, durant son stockage ou sa transmission ;

b) l'intégrité/l'authenticité : l'utilisation de signatures électroniques ou de codes d'authentification de message permet de vérifier l'authenticité ou l'intégrité de l'information sensible ou critique, durant son stockage ou sa transmission , l'utilisation d'algorithmes permettant de contrôler l'intégrité des fichiers ;

c) non-répudiation : l'utilisation de techniques cryptographiques permet d'apporter la preuve de la survenue ou de la non-survenue d'un événement ou d'une action ;

d) authentification : l'utilisation de techniques cryptographiques permet d'authentifier les utilisateurs et les autres entités système demandant un accès ou engageant une transaction avec des utilisateurs, des entités et des ressources du système.

Il convient que la décision d'utiliser une solution cryptographique s'inscrive dans le cadre d'un processus plus large d'appréciation du risque et de détermination des mesures nécessaires. Cette appréciation peut donc être utilisée pour déterminer la pertinence d'une mesure cryptographique, le type de mesure qu'il convient d'appliquer, dans quel but et pour quel processus métier.

Une politique portant sur le thème de l'utilisation de la cryptographie permet d'optimiser les avantages des techniques cryptographiques, de réduire au minimum les risques associés et d'éviter toute utilisation impropre ou incorrecte.

La gestion des clés cryptographiques est essentielle à l'efficacité des techniques cryptographiques. L'ISO/IEC 11770 (toutes les parties) donne des informations supplémentaires sur la gestion des clés.

Il est également possible d'utiliser des techniques cryptographiques pour protéger les clés cryptographiques.

8.25 Cycle de vie de développement sécurisé

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

Mesure de sécurité

Il convient de définir et d'appliquer des règles de développement sécurisé des logiciels et des systèmes.

Objectif

S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement sécurisé des logiciels et des systèmes.

Préconisations

Le développement sécurisé est une nécessité pour bâtir un service, une architecture, un logiciel et un système sécurisés. Pour y parvenir, il convient de prendre en compte les aspects suivants :

a) la séparation des environnements de développement, de test et de production (voir 8.31) ;

b) les recommandations liées à la sécurité dans le cycle de vie du développement d'un logiciel :

   1) la sécurité de la méthodologie de développement du logiciel (voir 8.28 et 8.27) ;

   2) les lignes directrices relatives à la sécurité du codage pour chaque langage de programmation utilisé (voir 8.28) ;

c) les exigences de sécurité dans les spécifications et la phase de conception (voir 5.8) ;

d) les points de contrôle de la sécurité aux différentes étapes clés du projet (voir 5.8) ;

e) les tests de la sécurité et du système, notamment essais de régression, analyse du code et tests de pénétration (voir 8.29) ;

f) les référentiels sécurisés pour le code source et la configuration (voir 8.4 et 8.9) ;

g) la sécurité dans le contrôle des versions (voir 8.32) ;

h) les connaissances et la formation requises concernant la sécurité des applications (voir 8.28) ;

i) la capacité des développeurs à éviter, découvrir et corriger les vulnérabilités (voir 8.28) ;

j) les exigences et alternatives à l'octroi de licence pour bénéficier de solutions rentables et éviter de futurs problèmes d'octroi de licence (voir 5.32).

Si le développement est externalisé, il convient que l'organisation obtienne l'assurance que l'éditeur se conforme aux règles de développement sécurisé de l'organisation (voir 8.30).

Informations supplémentaires

Des développements peuvent aussi s'opérer au sein d'applications telles que les applications bureautiques, la rédaction de scripts, les navigateurs et les bases de données.

8.26 Exigences de sécurité des applications

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection #Défense

Mesure de sécurité

Il convient d'identifier les exigences de sécurité de l'information, de les définir et de les approuver lors du développement ou de l'achat d'applications.

Objectif

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

Préconisations

Généralités

Il convient d'identifier les exigences de sécurité des applications et de les spécifier dans le cadre des exigences fonctionnelles et non fonctionnelles. Ces exigences sont généralement déterminées par le biais d'une appréciation du risque. Il convient d'élaborer les exigences avec l'appui de spécialistes en sécurité de l'information.

Les exigences de sécurité des applications peuvent couvrir un large éventail de thématiques, selon la finalité de l'application.

Il convient que les exigences de sécurité des applications comprennent, selon le cas :

a) le niveau de confiance dans l'identité des entités, par exemple via l'authentification (voir 5.17, 8.2, 8.5) ;

b) l'identification du type d'information et le niveau de classification à traiter par l'application ;

c) la nécessité de séparer l'accès et le niveau d'accès aux données et aux fonctions disponibles dans l'application ;

d) la résilience contre les attaques malveillantes ou les perturbations involontaires (par exemple, protection contre les débordements de la mémoire tampon ou les injections SQL) ;

e) les exigences légales, statutaires et réglementaires dans la juridiction où la transaction est générée, traitée, exécutée ou stockée ;

f) la nécessité de confidentialité des informations personnelles de toutes les parties impliquées ;

g) les exigences de protection de l'information confidentielle ;

h) la protection des données pendant leur traitement, en transit et au repos ;

i) la nécessité de chiffrer les communications de façon sécurisée entre toutes les parties concernées ;

j) les contrôles de saisie, y compris contrôles d'intégrité ;

k) les contrôles automatisés (par exemple, limites d'approbation ou doubles approbations) ;

l) les contrôles de sortie, prenant également en compte qui a accès aux sorties et l'autorisation correspondante ;

m) les restrictions liées au contenu des champs de « texte libre » dans la mesure où ceux-ci peuvent entraîner un stockage non contrôlé de données confidentielles (par exemple, à caractère personnel) ;

n) les exigences découlant du processus métier, telles que la journalisation et la surveillance des transactions, les exigences de non-répudiation ;

o) les exigences prescrites par les autres mesures de sécurité, telles que les interfaces pour la journalisation et la surveillance ou les systèmes de détection de fuite de données ;

p) le traitement des messages d'erreur.

Services transactionnels

En outre, pour les applications qui proposent des services transactionnels entre l'organisation et un partenaire, il convient de prendre en compte les éléments suivants lors de l'identification des exigences de sécurité de l'information :

a) le niveau de confiance requis par chaque partie en ce qui concerne l'identité déclarée des autres ;

b) le niveau de confiance requis concernant l'intégrité de l'information échangée ou traitée et les mécanismes d'identification du manque d'intégrité (par exemple, CRC, hachage, signatures numériques) ;

c) les processus d'autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels clés ;

d) la confidentialité, l'intégrité, la preuve de l'envoi et de la réception des documents-clés et la non-répudiation, par exemple concernant les contrats associés à des processus d'appel d'offres et de contrats ;

e) la confidentialité et l'intégrité de toutes transactions, par exemple commandes, coordonnées de livraison et confirmation de réception ;

f) les exigences concernant la durée pendant laquelle garder la transaction confidentielle ;

g) les exigences en termes d'assurance et autres exigences contractuelles.

Applications de commande et de paiement électroniques

En outre, pour les applications impliquant la passation de commande et le paiement électroniques, il convient de prendre en compte les éléments suivants :

a) les exigences concernant le maintien de la confidentialité et de l'intégrité des éléments du bon de commande ;

b) le degré de vérification adéquat pour contrôler les détails de paiement fournis par le client ;

c) le fait d'éviter la perte ou la duplication des détails de la transaction ;

d) le stockage des détails des transactions hors de tout environnement accessible au public, à l'instar d'une plateforme de stockage en place sur l'intranet de l'organisation, et le fait de ne pas les conserver ni les exposer sur un support de stockage directement accessible depuis Internet ;

e) que lorsqu'une autorité de confiance est utilisée (par exemple dans le but d'émettre et de tenir à jour des signatures ou des certificats électroniques), la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou des signatures.

Plusieurs des considérations qui précèdent peuvent être satisfaites par l'application de la cryptographie (voir 8.24), en tenant compte de la conformité aux exigences légales (voir 5.31 à 5.36, et voir notamment 5.31 pour la législation en matière de cryptographie).

Informations supplémentaires

Les applications accessibles à partir de réseaux sont exposées à toute une série de menaces associées aux réseaux, telles que les activités frauduleuses, les différends contractuels ou la divulgation d'information au grand public ; transmission incomplète, erreurs d'acheminement, modification non autorisée, duplication non autorisée ou réémission du message. Par conséquent, il est indispensable de procéder à des appréciations détaillées des risques et de déterminer avec soin les mesures de sécurité. Les mesures exigées incluent souvent des méthodes de cryptographie pour l'authentification et la sécurisation des transferts de données.

De plus amples informations sur la sécurité des applications sont disponibles dans l'ISO/IEC 27034 (toutes les parties).

8.27 Principes d'ingénierie et d'architecture système sécurisée

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

Mesure de sécurité

Il convient d'établir, de documenter, de tenir à jour et d'appliquer des principes d'ingénierie de la sécurité des systèmes à toutes les activités de développement de systèmes d'information.

Objectif

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

Préconisations

Il convient d'établir, de documenter et d'appliquer des principes d'ingénierie de la sécurité aux activités d'ingénierie de systèmes d'information. Il convient de concevoir la sécurité dans toutes les couches de l'architecture (activité, données, applications et technologie). Il convient d'analyser les nouvelles technologies au regard des risques de sécurité et il convient de revoir la conception par rapport aux modèles d'attaques connus.

Les principes d'ingénierie sécurisée proposent des recommandations sur les techniques d'authentification de l'utilisateur, les contrôles de session sécurisés et la validation des données, le nettoyage et l'élimination des codes de débogage.

Il convient que les principes d'ingénierie de la sécurité des systèmes prévoient l'analyse :

a) de la totalité des mesures de sécurité requises pour protéger l'information et les systèmes contre les menaces identifiées (par exemple, politiques portant sur des thèmes, méthodes, procédures, dispositifs ou mécanismes programmés) ;

b) de la capacité des mesures de sécurité à prévenir les événements de sécurité, à les détecter ou à y répondre ;

c) des mesures de sécurité spécifiques exigées par certains processus métier (par exemple, chiffrement de l'information sensible, contrôle de l'intégrité et signature numérique de l'information) ;

d) de l'emplacement et de la façon dont les mesures de sécurité doivent être appliquées (par exemple, via l'intégration à une architecture de sécurité et l'infrastructure technique) ;

e) de la façon dont les mesures de sécurité (manuelles et automatisées) fonctionnent conjointement pour produire un ensemble intégré de mesures.

Il convient que les principes d'ingénierie de la sécurité prennent en compte :

a) la nécessité d'intégration à une architecture de sécurité ;

b) l'infrastructure de sécurité technique, par exemple l'infrastructure de clé publique (ou infrastructure PKI pour Public Key Infrastructure), la gestion des identités et des accès (ou IAM pour Identity and access management), la prévention de la fuite de données et la gestion des accès dynamiques ;

c) la capacité de l'organisation à développer et à supporter la technologie choisie ;

d) le coût, le temps et la complexité qu'implique la prise en compte des exigences en matière de sécurité ;

e) les bonnes pratiques actuelles.

Il convient que l'ingénierie de la sécurité des systèmes implique :

a) l'application des principes de l'architecture de sécurité, notamment « sécurité dès le stade de la conception », « défense en profondeur », « sécurité par défaut », « refus par défaut », « sécurité intégrée », « défiance à l'égard des données d'entrée des applications externes », « sécurité du déploiement », « présumer la compromission », « facilité d'utilisation et de gestion » et « moindre fonctionnalité » ;

b) une revue de la conception orientée sécurité pour permettre d'identifier les vulnérabilités en termes de sécurité de l'information, s'assurer que les mesures de sécurité sont spécifiées et satisfaire aux exigences en matière de sécurité ;

c) la documentation et la reconnaissance formelle des mesures de sécurité qui ne satisfont pas aux exigences (par exemple, en raison du contournement des exigences de sécurité).

Il convient que l'organisation envisage un modèle de principes d'ingénierie de la sécurité intégrant la protection des ressources, avec des concepts tels que les suivants :

a) supposer que les systèmes d'information de l'organisation sont déjà compromis et ne pas se reposer sur la seule sécurité du périmètre du réseau ;

b) employer une approche du type « ne jamais faire confiance, toujours vérifier » pour l'accès aux systèmes d'information ;

c) s'assurer que les demandes adressées aux systèmes d'information sont chiffrées de bout en bout ;

d) vérifier chaque demande adressée aux systèmes d'information comme si elle provenait d'un réseau externe ouvert, même si cette demande provient de l'intérieur de l'organisation ;

e) utiliser des droits d'accès basés sur le principe du moindre privilège et des techniques de contrôle d'accès telles que l'accès juste à temps ou juste suffisant (voir 5.18 et 8.2) ;

f) toujours authentifier et autoriser les demandes adressées aux systèmes d'information par rapport à l'information, notamment données d'authentification (voir 5.17) et identités utilisateur (5.16), données relatives au terminal final de l'utilisateur et classification des données (voir 5.12).

S'il y a lieu, il convient d'appliquer les principes d'ingénierie de la sécurité au développement externalisé de systèmes d'information par le biais de contrats et autres accords exécutoires passés entre l'organisation et le prestataire auprès duquel l'organisation externalise le développement. Il convient que l'organisation confirme que les principes d'ingénierie de la sécurité du prestataire ont la même rigueur que ses propres principes.

Il convient de revoir régulièrement les principes d'ingénierie de la sécurité et les procédures d'ingénierie établies pour s'assurer qu'ils contribuent de manière efficace à l'amélioration des normes de sécurité liées au processus d'ingénierie. Il convient également de les revoir régulièrement pour s'assurer qu'ils restent d'actualité pour combattre toute nouvelle menace potentielle et continuent de s'appliquer aux avancées réalisées dans les technologies et les solutions appliquées.

Informations supplémentaires

Les principes d'ingénierie de la sécurité peuvent être appliqués à la conception ou à la configuration de différentes techniques, notamment :

a) tolérance aux pannes ;

b) cloisonnement (par exemple via la virtualisation ou la conteneurisation) ;

c) inviolabilité.

Le code d'application est mieux conçu en partant de l'hypothèse qu'il est toujours exposé à une attaque, que celle-ci résulte d'une erreur ou d'un acte malveillant. En outre, les applications critiques peuvent être conçues avec une tolérance aux pannes internes. Par exemple, le résultat en sortie d'un algorithme complexe peut être contrôlé pour vérifier qu'il s'inscrit dans des limites sûres avant que les données ne soient utilisées dans une application critique sur le plan financier ou de la sécurité, par exemple. Le code qui exécute le contrôle des limites est simple et il est donc plus facile de prouver l'exactitude.

Certaines applications Web sont sujettes à toute une série de vulnérabilités qui découlent d'insuffisances au niveau de la conception ou du codage, comme les attaques XSS (« Cross-site scripting ») et par injection dans la base de données. Dans les attaques de ce type, les demandes peuvent être manipulées pour utiliser abusivement la fonctionnalité du serveur Web.

Une organisation peut recourir à des techniques de virtualisation sécurisée pour éviter toute interférence entre les applications qui tournent sur un même dispositif physique. Si une instance virtuelle d'une application est compromise par un attaquant, seule cette instance est affectée. L'attaque n'a aucun effet sur les autres applications ou données.

Des techniques d'inviolabilité peuvent être utilisées pour détecter les manipulations de conteneurs d'information, aussi bien physiques (par exemple, alarme anti-effraction) que logiques (par exemple, fichier de données). Ces techniques se caractérisent par l'existence d'un enregistrement de la tentative de manipulation du conteneur. En outre, la mesure peut empêcher l'extraction des données par le biais de leur destruction (la mémoire du dispositif peut, par exemple, être effacée).

L'ISO/IEC 27040 donne des conseils plus détaillés sur la façon de concevoir et configurer les systèmes de stockage réseau, à suivre dans le cas de données très sensibles, telles que les données médicales des patients.

8.28 Codage sécurisé

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

Mesure de sécurité

Il convient d'appliquer des principes de codage sécurisé au développement de logiciels.

Objectif

S'assurer que le logiciel est développé dans un souci de sécurité et réduire ainsi le nombre de vulnérabilités potentielles du logiciel en termes de sécurité de l'information.

Préconisations

Généralités

Il convient de définir des processus à l'échelle de l'organisation pour s'assurer de la bonne gouvernance du codage sécurisé. Il convient d'établir et d'appliquer une base de référence de sécurité minimale. En outre, il convient d'étendre ces processus et cette gouvernance aux composantes logicielles de provenance externe et de type ouvert (« open source »).

Il convient que l'organisation surveille les menaces du monde réel et les conseils actualisés, ainsi que les informations sur les vulnérabilités logicielles, pour orienter ses principes de codage sécurisé en s'appuyant sur l'amélioration et l'apprentissage continus. Cela peut contribuer à garantir la mise en œuvre de pratiques de codage sécurisé efficaces pour contrer les menaces en constante évolution.

Planification et prérequis du codage

Il convient d'appliquer les principes de codage sécurisé aux nouveaux développements et aux scénarios de réutilisation. Il convient d'appliquer ces principes aux activités de développement aussi bien à l'intérieur de l'organisation que pour les produits et services fournis par l'organisation à des tiers. Il convient que la planification et les prérequis du codage tiennent compte des éléments suivants :

a) attentes et principes approuvés de l'organisation en matière de codage sécurisé, à appliquer aux développements effectués en interne et externalisés ;

b) pratiques de codage courantes et historiques entraînant des vulnérabilités en termes de sécurité de l'information ;

c) configuration d'outils de développement, tels que les environnements de développement intégré (ou IDE pour Integrated development environment), pour faciliter la création de code sécurisé ;

d) respect des recommandations émises par les fournisseurs d'outils de développement et d'environnements d'exécution, le cas échéant ;

e) maintenance et utilisation d'outils de développement mis à jour (tels que les compilateurs) ;

f) qualification des développeurs en matière de création de code sécurisé ;

g) conception et architecture sécurisées, y compris modélisation des menaces ;

h) normes de codage sécurisé et, le cas échéant, obligation de les utiliser ;

i) utilisation d'environnements contrôlés pour le développement.

Pendant le codage

Il convient de tenir compte des éléments suivants pendant le codage :

a) pratiques de codage sécurisé spécifiques des langages de programmation et techniques utilisés ;

b) utilisation de techniques de programmation sécurisée, telles que la programmation en binôme, la restructuration, la revue par des pairs, itérations de sécurité et développement piloté par les tests ;

c) utilisation de techniques de programmation structurées ;

d) documentation du code et élimination des défauts de programmation pouvant permettre l'exploitation de vulnérabilités en termes de sécurité de l'information ;

e) interdiction d'utiliser des techniques de conception non sécurisées (par exemple, mots de passe codés en dur, échantillons de code non approuvés et services Web non authentifiés).

Il convient de réaliser des tests pendant et après le développement (voir 8.29). Les processus de test des applications de sécurité statiques (ou processus SAST pour Static application security testing) permettent d'identifier les vulnérabilités des logiciels.

Avant de rendre un logiciel opérationnel, il convient d'évaluer les points suivants :

a) la surface d'attaque et le principe du moindre privilège ;

b) la réalisation d'une analyse des erreurs de programmation les plus courantes et la documentation de leur atténuation.

Revue et maintenance

Une fois que le code a été rendu opérationnel :

a) il convient d'assembler et de déployer les mises à jour de façon sécurisée ;

b) il convient de traiter les vulnérabilités signalées en matière de sécurité de l'information (voir 8.8) ;

c) il convient de journaliser les erreurs et les attaques suspectées et de passer régulièrement les journaux en revue pour apporter des ajustements au code, si besoin ;

d) il convient de protéger le code source contre tout accès non autorisé et toute altération (par exemple en recourant à des outils de gestion de la configuration, qui comportent généralement des fonctions du type contrôle d'accès et contrôle des versions).

En cas d'utilisation d'outils et de bibliothèques externes, il convient que l'organisation considère les points suivants :

a) s'assurer que les bibliothèques externes sont gérées et régulièrement mises à jour avec des cycles de versions. Gérer un inventaire des bibliothèques utilisées et de leurs versions ;

b) sélection, autorisation et réutilisation des composants passés en revue, en particulier les composants d'authentification et de cryptographie ;

c) licence, sécurité et historique des composants externes ;

d) assurance que le logiciel peut être soumis à une maintenance et à un suivi et qu'il provient de sources fiables et éprouvées ;

e) disponibilité suffisante sur le long terme des ressources et artefacts de développement.

Lorsqu'une modification du progiciel est nécessaire, il convient de tenir compte des points suivants :

a) le risque de compromettre les commandes intégrées et le processus de vérification de l'intégrité ;

b) le fait d'obtenir ou non le consentement de l'éditeur ;

c) la possibilité d'obtenir les changements souhaités auprès de l'éditeur, sous la forme de mises à jour de programme classiques ;

d) les conséquences si l'organisation devenait responsable de la maintenance du logiciel suite à des changements ;

e) la compatibilité avec les autres logiciels en service.

Informations supplémentaires

Un principe directeur veut que l'on s'assure que le code sécurisé pertinent est appelé lorsque cela est nécessaire et qu'il est inviolable. Les programmes installés à partir de code binaire compilé présenteront également ces propriétés, mais uniquement pour les données conservées dans l'application. Pour les langages interprétés, le concept fonctionnera uniquement lors de l'exécution du code sur un serveur autrement inaccessible par les utilisateurs et autres processus qui l'utilisent et dont les données sont conservées dans une base de données bénéficiant d'une protection similaire. Par exemple, le code interprété peut être exécuté dans un service en nuage dans lequel l'accès au code lui-même requiert des privilèges d'administration. Il convient de protéger ce type d'accès administrateur par des mécanismes tels que les principes d'administration juste-à-temps (voir 5.18) et des clés Secure Shell (ou clés SSH). Si le propriétaire de l'application a accès aux scripts par accès distant direct au serveur, il en va logiquement de même pour un attaquant. Dans de tels cas, il convient de configurer les serveurs Web de sorte à empêcher la navigation dans les répertoires.

De plus amples informations sur l'évaluation de la sécurité des TIC sont disponibles dans l'ISO/IEC 15408 (toutes les parties).

8.29 Tests de sécurité dans le développement et l'acceptation

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

Mesure de sécurité

Il convient de définir des processus pour les tests de sécurité et de les mettre en œuvre au cours du cycle de développement.

Objectif

Valider le respect des exigences de sécurité de l'information lors du déploiement dans l'environnement de production.

Préconisations

Il convient de tester et de vérifier en profondeur les nouveaux systèmes d'information, les mises à niveau et les nouvelles versions au cours des processus de développement. Il convient d'intégrer pleinement les tests de sécurité aux tests portant sur le système ou les composants.

Il convient de mener les tests de sécurité en référence à un ensemble d'exigences pouvant être exprimées comme fonctionnelles ou non fonctionnelles. Il convient que les tests de sécurité portent sur :

a) les fonctions de sécurité telles que l'authentification utilisateur (voir 8.5), les restrictions d'accès (voir 8.3) et l'utilisation de la cryptographie (voir 8.24) ;

b) le codage sécurisé (voir 8.28) ;

c) les configurations sécurisées (voir 8.9, 8.20 et 8.23) y compris celles des systèmes d'exploitation, des pare-feu et autres composants de sécurité.

Il convient de déterminer des plans de test à l'aide d'un ensemble de critères. Il convient de définir l'étendue des tests proportionnellement à l'importance, la nature du système et l'impact potentiel du changement introduit. Il convient que le plan de test comporte :

a) un programme détaillé des activités et des tests ;

b) les données d'entrée, avec les résultats attendus en sortie sous un certain nombre de conditions ;

c) les critères permettant d'évaluer les résultats ;

d) la décision prise concernant les actions à suivre, si besoin.

L'organisation peut recourir à des outils automatiques, tels que des outils d'analyse de code ou des scanneurs de vulnérabilités. Il convient qu'elle vérifie les actions correctives apportées aux défauts liés à la sécurité.

En ce qui concerne les développements in situ, il convient que ces tests soient réalisés dès le début par l'équipe de développement. Il convient ensuite de procéder à des tests de conformité indépendants pour s'assurer que le système fonctionne comme prévu et uniquement comme prévu (voir 5.8 et 8.29). Il convient de considérer les éléments suivants :

a) exécuter des tâches de revue de code pour tester les anomalies de sécurité, notamment les saisies et conditions non anticipées ;

b) exécuter une analyse des vulnérabilités pour identifier les configurations non sécurisées et les vulnérabilités du système ;

c) exécuter des tests de pénétration pour identifier le code et les éléments de conception non sécurisés.

Dans le cas d'un développement externalisé et de l'achat de composants, il convient de suivre une procédure d'achat. Dans les contrats conclus avec le fournisseur, il convient de traiter les exigences de sécurité identifiées (voir 5.20). Il convient d'évaluer les produits et les services au regard de ces critères avant de procéder à l'achat.

Il convient de réaliser les tests dans un environnement de test ressemblant le plus possible à l'environnement de production cible pour garantir que le système n'introduira pas de vulnérabilités dans l'environnement de l'organisation et que les tests seront fiables (voir 8.31).

Informations supplémentaires

Il est possible de mettre en place plusieurs environnements de test pouvant être utilisés pour réaliser différents types de tests (par exemple, tests fonctionnels et de performance). Ces différents environnements peuvent être virtuels, avec des configurations individuelles pour simuler plusieurs environnements d'exploitation.

Les tests et la surveillance des environnements, outils et technologies de test doivent également être pris en compte pour garantir l'efficacité des tests. Il en va de même pour la surveillance des systèmes de surveillance déployés dans les paramètres de développement, de test et de production. Il convient de déterminer, en fonction de la sensibilité des systèmes et des données, le nombre de couches de métatest nécessaire.

8.30 Développement externalisé

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection #Détection	#Sécurité_système_et_réseau #Sécurité_des_applications #Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient que l'organisation dirige, contrôle et passe en revue les activités liées au développement du système externalisé.

Objectif

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

Préconisations

Si le développement du système est externalisé, il convient que l'organisation communique et établisse des exigences et des attentes, et qu'elle contrôle et vérifie de façon continue si la livraison des travaux externalisés répond à ces attentes. Il convient de considérer les aspects suivants au sein de la chaîne d'approvisionnement externe de l'organisation :

a) accords de licence, propriété du code et droits de propriété intellectuelle relatifs au contenu externalisé (voir 5.32) ;

b) exigences contractuelles relatives à la conception sécurisée, au codage et aux pratiques de tests (voir 8.25 à 8.29) ;

c) fourniture au développeur prestataire du modèle des menaces approuvé ;

d) test de conformité de la qualité et de la précision des livrables (voir 8.29) ;

e) communication des preuves montrant que les niveaux minimaux acceptables de sécurité et les capacités en matière de protection de la vie privée sont établis, par exemple rapports d'assurance ;

f) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de contenus volontairement ou involontairement malveillants à la livraison ;

g) communication des preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de vulnérabilités connues ;

h) accords de séquestre concernant le code source du logiciel, par exemple si le fournisseur cesse son activité ;

i) droit contractuel de procéder à un audit des processus et des contrôles de développement ;

j) exigences de sécurité relatives à l'environnement de développement (voir 8.31) ;

k) l'organisation demeure responsable de la conformité aux lois en vigueur.

Informations supplémentaires

De plus amples informations sur les relations avec les fournisseurs sont disponibles dans l'ISO/IEC 27036 (toutes les parties).

8.31 Séparation des environnements de développement, de test et de production

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

Mesure de sécurité

Il convient de séparer et de sécuriser les environnements de développement, de test et de production.

Objectif

Protéger l'environnement de production et les données correspondantes de toute compromission par les activités de développement et de test.

Préconisations

Il convient de déterminer et de mettre en œuvre un niveau de séparation entre les environnements de développement, de test et de production pour prévenir les problèmes en mode productif.

Il convient d'envisager les éléments suivants :

a) séparer de façon adéquate les systèmes de développement et de production et les exploiter dans des domaines différents, par exemple dans des environnements physiques ou virtuels distincts ;

b) définir et documenter les règles et autorisations relatives au déploiement du logiciel depuis le développement jusqu'à la production ;

c) tester les modifications apportées aux systèmes et aux applications de production dans un environnement de test ou de préproduction avant de les appliquer aux systèmes de production (voir 8.29) ;

d) en dehors de circonstances exceptionnelles, ne pas procéder à des tests dans des environnements de production ;

e) rendre inaccessibles les compilateurs, éditeurs et autres outils de développement ou programmes utilitaires depuis les systèmes de production lorsqu'ils ne sont pas nécessaires ;

f) afficher les étiquettes d'identification de l'environnement appropriées dans les menus afin de limiter les risques d'erreur ;

g) ne pas copier d'information sensible dans les environnements des systèmes de développement et de test sauf si des mesures équivalentes sont prévues pour les systèmes de développement et de test.

Dans tous les cas, il convient de protéger les environnements de développement et de test en prenant en compte les points suivants :

a) application de correctifs et de mises à jour sur tous les outils de développement, d'intégration et de test (y compris les générateurs, intégrateurs, compilateurs, systèmes de configuration et bibliothèques) ;

b) configuration sécurisée des systèmes et du logiciel ;

c) contrôle de l'accès aux environnements ;

d) surveillance des changements apportés à l'environnement et au code qu'il renferme ;

e) surveillance de la sécurité des environnements.

Dans certains cas, la distinction entre les environnements de développement, de test et de production peut être volontairement floue ; les tests sont alors exécutés dans un environnement de développement ou via des déploiements contrôlés à destination d'utilisateurs ou de serveurs opérationnels (par exemple, un petit nombre d'utilisateurs pilotes). Dans certains cas, les tests du produit peuvent avoir lieu via l'utilisation du produit en mode productif au sein de l'organisation. Il convient de définir des processus pour passer de la phase de développement à la phase de test et inversement. En outre, pour réduire les temps d'arrêt liés aux déploiements en mode productif, deux environnements de production identiques peuvent être pris en charge, dont un seul est opérationnel à un instant t.

Il convient qu'une personne seule n'ait pas la possibilité d'apporter de changements au niveau du développement et de la production sans revue et approbation préalables. Cela peut, par exemple, être assuré par la séparation des droits d'accès ou via des règles soumises à un contrôle. Dans des situations exceptionnelles, il convient de mettre en œuvre des mesures supplémentaires telles qu'une journalisation détaillée et une surveillance en temps réel pour détecter tout changement non autorisé et agir en conséquence.

Informations supplémentaires

Les activités de développement et de test peuvent causer de graves problèmes, tels qu'une modification indésirable des fichiers ou de l'environnement système, ou une défaillance du système. Il est nécessaire de maintenir un environnement stable et connu de tous permettant de réaliser des tests significatifs et d'empêcher tout accès inapproprié des développeurs à l'environnement de production.

Sans l'application de mesures et procédures adéquates, les développeurs et les testeurs qui ont accès aux systèmes de production peuvent introduire des risques importants. Parmi les risques figurent l'exécution de code non autorisé et non testé dans les systèmes de production, la divulgation de données confidentielles et les problèmes liés à la disponibilité et à l'intégrité des données.

Les mesures et procédures englobent la définition précise des rôles parallèlement à la mise en œuvre d'exigences de séparation des tâches et la mise en place de processus de surveillance adéquats.

Les développeurs et les personnes chargées des tests représentent également une menace pour la confidentialité de l'information en mode productif. Les activités de développement et de test peuvent entraîner des changements involontaires dans les logiciels ou l'information si elles partagent le même environnement informatique. La séparation physique des environnements de développement, de test et de production est donc souhaitable pour réduire les risques de changements accidentels ou d'accès non autorisé aux logiciels en production et aux données liées à l'activité (voir 8.33 pour la protection des informations de test).

8.32 Gestion des changements

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

Mesure de sécurité

Il convient que les changements apportés aux moyens de traitement de l'information et à l'information soient soumis à des procédures de gestion des changements.

Objectif

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

Préconisations

Il convient que l'introduction de nouveaux systèmes et les changements de grande ampleur apportés aux systèmes existants suivent les règles établies et une procédure formelle de documentation, de spécification, de phase de tests, de contrôle qualité et de mise en œuvre. Il convient de mettre en place des responsabilités et des procédures de management pour assurer un contrôle satisfaisant de tous les changements apportés.

Il convient de documenter les procédures de contrôle des changements et de les appliquer afin de garantir la confidentialité, l'intégrité et la disponibilité de l'information dans les moyens de traitement de l'information et les systèmes d'information, d'un bout à l'autre du cycle de développement du système, depuis les étapes de conception initiales jusqu'aux travaux de maintenance ultérieurs.

Dans la mesure du possible, il convient d'intégrer les procédures de contrôle des changements relatives à l'infrastructure et aux logiciels TIC.

Il convient d'intégrer les éléments suivants aux procédures de contrôle des changements :

a) planification et évaluation de l'impact potentiel des changements en prenant en compte toutes les dépendances ;

b) communication des changements aux parties intéressées ;

c) preuves des tests et acceptation des tests relatifs aux changements (voir 8.29) ;

d) autorisation des changements ;

e) mise en œuvre des changements, y compris plans de déploiement ;

f) questions liées aux notions d'urgence et de secours, notamment procédures de repli ;

g) tenue à jour d'enregistrements des changements, comprenant tout ce qui précède ;

h) adaptation de la documentation relative à l'exploitation (voir 5.37) et aux procédures utilisateurs en fonction des changements ;

i) adaptation des plans de continuité des TIC et des procédures de réponse et de récupération (voir 5.30) en fonction des changements.

Informations supplémentaires

Un contrôle insuffisant des changements apportés aux moyens de traitement de l'information et aux systèmes d'information constitue une cause répandue de défaillance du système ou de la sécurité. Les changements apportés à l'environnement de production, particulièrement s'il s'agit de faire passer un logiciel du stade de développement au stade d'exploitation, peuvent avoir des conséquences sur l'intégrité et la disponibilité des applications.

Un changement apporté à un logiciel peut avoir une incidence sur l'environnement de production et inversement.

Les bonnes pratiques prévoient que la phase de test des composants de TIC soit réalisée dans un environnement séparé des environnements de développement et de production (voir 8.31). Ce cloisonnement permet de contrôler le nouveau logiciel et d'ajouter une protection supplémentaire aux informations d'exploitation utilisées dans le cadre des tests. Il convient que ces dispositions intègrent les correctifs logiciels, les « service packs » (ensembles de modifications provisoires) et autres mises à jour.

L'environnement de production comprend les systèmes d'exploitation, les bases de données et les logiciels médiateurs. Il convient que la mesure s'applique aux changements apportés aux applications et aux infrastructures.

8.33 Informations relatives aux tests

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

Mesure de sécurité

Il convient de sélectionner, de protéger et de gérer les informations relatives aux tests.

Objectif

Garantir la pertinence des tests et la protection des informations opérationnelles utilisées dans le cadre des tests.

Préconisations

Il convient de sélectionner les informations relatives aux tests pour s'assurer de la fiabilité des résultats des tests et de la confidentialité des informations opérationnelles qui en relèvent. Il convient de ne pas copier d'information sensible (notamment des données à caractère personnel) dans les environnements de développement et de test (voir 8.31).

Lorsque des copies d'informations opérationnelles sont utilisées pour les besoins d'un test, il convient d'appliquer les lignes directrices suivantes afin de les protéger :

a) appliquer les procédures de contrôle d'accès qui s'appliquent aux systèmes d'applications opérationnels, également aux systèmes d'applications de test ;

b) obtenir une nouvelle autorisation chaque fois qu'une information opérationnelle est copiée dans un environnement de test ;

c) journaliser toute reproduction et utilisation d'information opérationnelle, afin de créer un système de traçabilité ;

d) si de l'information sensible doit être utilisée pour les besoins d'un test, la protéger par une technique de retrait ou de modification (voir 8.11) ;

e) supprimer correctement (voir 8.10) toute information opérationnelle de l'environnement de test immédiatement après la fin des tests pour éviter l'utilisation non autorisée d'information relative aux tests.

Il convient de stocker les informations relatives aux tests de façon sécurisée (pour éviter toute altération susceptible d'engendrer des résultats non valides) et de les utiliser uniquement dans le cadre des tests.

Si l'environnement de test repose sur un service en nuage, il convient de le supprimer une fois que le test est achevé.

Informations supplémentaires

Les tests de système et de conformité peuvent nécessiter d'importants volumes d'informations de test qui soient aussi représentatives que possible des informations opérationnelles.

8.34 Protection des systèmes d'information en cours d'audit et de test

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau #Protection_des_informations	#Gouvernance_et_écosystème #Protection

Mesure de sécurité

Il convient que les tests d'audit et autres activités d'assurance faisant intervenir une évaluation des systèmes opérationnels soient planifiés et fassent l'objet d'un accord entre le testeur et le niveau de direction approprié.

Objectif

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

Préconisations

Il convient de respecter les points suivants :

a) arrêter avec le niveau de direction approprié les demandes d'audit liées à l'accès aux systèmes et aux données ;

b) définir le périmètre des tests techniques d'audit et le contrôler ;

c) limiter les tests d'audit à un accès en lecture seule aux logiciels et aux données. Si l'accès en lecture n'est pas disponible pour obtenir l'information nécessaire, faire réaliser le test par un administrateur expérimenté bénéficiant des droits d'accès nécessaires, pour le compte de l'auditeur ;

d) si l'accès est accordé, établir et vérifier les exigences de sécurité (par exemple, antivirus et application de correctifs) des dispositifs utilisés pour accéder aux systèmes (par exemple, ordinateurs portables ou tablettes) avant d'autoriser l'accès ;

e) n'autoriser les accès autres qu'en lecture seule que pour les copies isolées de fichiers système. Une fois l'audit terminé, il convient soit de les supprimer, soit de les protéger de manière appropriée si les exigences de documentation de l'audit imposent de les conserver ;

f) identifier et définir les demandes de traitement spécial ou additionnel, comme l'exécution d'outils d'audit ;

g) exécuter les tests d'audit pouvant compromettre la disponibilité du système en dehors des heures de travail ;

h) surveiller et journaliser tous les accès pour des besoins d'audit et de test.

Informations supplémentaires

L'impact sur les autres activités non opérationnelles doit également être pris en compte lors de l'étude de l'impact des activités de test et d'audit.C075652efig2.EPS

Annexe A
(informative)

Utilisation des attributs

A.1 Introduction

Cette annexe contient un tableau qui présente l'utilisation des attributs dans le but de créer différentes vues des mesures de sécurité. Des exemples d'utilisation de ces attributs sont proposés ci-dessous :

a) Types de mesures de sécurité (#Prévention, #Détection, #Correction)

Cet attribut peut être utilisé dans le cas où l'organisation souhaite contrôler l'équilibre des mesures déterminées, par exemple, si les mesures adéquates pour détecter les événements liés à la sécurité de l'information sont déterminées, et pas uniquement les mesures visant à prévenir les incidents liés à la sécurité de l'information.

b) Propriétés de sécurité de l'information (#Confidentialité, #Intégrité, #Disponibilité)

Cet attribut peut être utilisé dans le cas où l'organisation souhaite comprendre les propriétés de chaque mesure, par exemple, savoir si une mesure contribue à préserver toute la confidentialité, l'intégrité et la disponibilité de l'information ou si elle contribue seulement à une ou deux de ces propriétés.

c) Concepts de cybersécurité (#Identification, #Protection, #Détection, #Traitement, #Récupération)

Cet attribut peut être utilisé dans le cas où l'organisation établit à la fois un système de management de la sécurité de l'information (SMSI) et un cadre de cybersécurité en son sein, et qu'elle souhaite connaître la pertinence entre les mesures relatives au SMSI décrites dans le présent document et cinq concepts du cadre de cybersécurité décrit dans l'ISO/IEC TS 27101.

d) Capacités opérationnelles (#Gouvernance, #Gestion_des_actifs, #Protection_des_informations, #Sécurité_des_ressources_humaines, #Sécurité_physique, #Sécurité_système_et_réseau, #Sécurité_des_applications, #Configuration_sécurisée, #Gestion_des_identités_et_des_accès, #Gestion_des_menaces_et_des_vulnérabilités, #Continuité, #Sécurité_des_relations_fournisseurs, #Législation_et_conformité, #Gestion_des_événements_de_sécurité_de_l'information, #Assurance_de_sécurité_de_l'information)

Cet attribut peut être utilisé dans le cas où l'organisation souhaite classifier les mesures du point de vue qu'a le praticien et, par exemple, lorsque l'organisation souhaite affecter les services responsables en fonction de ces valeurs d'attributs.

e) Domaines de sécurité (#Gouvernance_et_écosystème, #Protection, #Défense, #Résilience)

Cet attribut peut être utilisé dans le cas où l'organisation souhaite classifier les mesures du point de vue des domaines, de l'expertise, des services et des produits relatifs à la sécurité de l'information.

Le Tableau A.1 contient une matrice de toutes les mesures qui figurent dans le présent document avec les valeurs d'attributs correspondantes.

Le filtrage ou le tri de la matrice peut être opéré à l'aide d'un outil tel qu'un simple tableur ou une base de données, pouvant comprendre des informations additionnelles comme le texte de la mesure, les préconisations, les recommandations ou les attributs spécifiques de l'organisation (voir A.2).

Tableau A.1 — Matrice des mesures et valeurs d'attributs

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.1	Politiques de sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Résilience
5.2	Fonctions et responsabilités liées à la sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Protection #Résilience
5.3	Séparation des tâches	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gouvernance	#Gouvernance_et_écosystème
5.4	Responsabilités de la direction	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème
5.5	Relations avec les autorités	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense #Résilience
5.6	Relations avec des groupes de travail spécialisés	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense
5.7	Intelligence des menaces	#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Identification #Détection	#Gestion_des_menaces_et_des_vulnérabilités	#Défense #Résilience
5.8	Sécurité de l'information dans la gestion de projet	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Gouvernance	#Gouvernance_et_écosystème #Protection
5.9	Inventaire des informations et des autres actifs associés	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gestion_des_actifs	#Gouvernance_et_écosystème #Protection
5.10	Utilisation correcte de l'information et des actifs associés	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Gouvernance_et_écosystème #Protection
5.11	Restitution des actifs	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs	#Protection
5.12	Classification de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Protection_des_informations	#Protection #Défense
5.13	Marquage des informations	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Protection_des_informations	#Défense

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.14	Transfert de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Protection
5.15	Contrôle d'accès	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection
5.16	Gestion des identités	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection
5.17	Informations d'authentification	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Gouvernance_et_écosystème #Protection
5.18	Droits d'accès	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection
5.19	Sécurité de l'information dans les relations avec les fournisseurs	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection
5.20	Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection
5.21	Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection
5.22	Suivi, revue et gestion des changements des services fournisseurs	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection #Défense
5.23	Sécurité de l'information dans l'utilisation de services en nuage	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection
5.24	Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information	#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.25	Appréciation des événements liés à la sécurité de l'information et prise de décision	#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.26	Réponse aux incidents liés à la sécurité de l'information	#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.27	Tirer des enseignements des incidents liés à la sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection #Identification	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.28	Recueil de preuves	#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.29	Sécurité de l'information durant une perturbation	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Continuité	#Protection #Résilience
5.30	Préparation des TIC pour la continuité d'activité	#Protection #Correction	#Disponibilité	#Protection #Traitement	#Continuité	#Protection #Résilience
5.31	Identification des exigences légales, statutaires, réglementaires et contractuelles	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Législation_et_conformité	#Gouvernance_et_écosystème #Protection
5.32	Droits de propriété intellectuelle	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Législation_et_conformité	#Gouvernance_et_écosystème
5.33	Protection des enregistrements	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Législation_et_conformité #Gestion_des_actifs #Protection_des_informations	#Défense
5.34	Vie privée et protection des DCP	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Protection_des_informations #Législation_et_conformité	#Protection
5.35	Revue indépendante de la sécurité de l'information	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Identification	#Assurance_de_sécurité_de_l'information	#Gouvernance_et_écosystème

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.36	Conformité aux politiques et normes de sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Législation_et_conformité	#Gouvernance_et_écosystème
5.37	Procédures d'exploitation documentées	#Prévention	#Disponibilité #Confidentialité #Intégrité	#Protection	#Continuité #Gestion_des_actifs #Sécurité_physique #Sécurité_système_et_réseau	#Gouvernance_et_écosystème #Protection #Défense
6.1	Présélection	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème
6.2	Conditions générales d'embauche	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème
6.3	Sensibilisation, apprentissage et formation à la sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème
6.4	Processus disciplinaire	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème
6.5	Responsabilités consécutivement à la fin ou à la modification du contrat de travail	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_ressources_humaines #Gestion_des_actifs	#Gouvernance_et_écosystème
6.6	Engagements de confidentialité ou de non-divulgation	#Prévention	#Confidentialité	#Protection	#Sécurité_des_ressources_humaines #Protection_des_informations #Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème
6.7	Travail à distance	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Sécurité_système_et_réseau #Sécurité_physique	#Gouvernance_et_écosystème #Protection
6.8	Signalement des événements liés à la sécurité de l'information	#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
7.1	Périmètre de sécurité physique	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection
7.2	Contrôles physiques des accès	#Prévention	#Intégrité #Disponibilité #Confidentialité	#Protection	#Sécurité_physique	#Protection

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
7.3	Sécurisation des bureaux, des salles et des équipements	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection
7.4	Surveillance de la sécurité physique	#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Sécurité_physique	#Protection
7.5	Protection contre les menaces physiques et environnementa-les	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection
7.6	Travail dans les zones sécurisées	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique	#Protection
7.7	Bureau propre et écran vide	#Prévention	#Confidentialité	#Protection	#Sécurité_physique	#Protection
7.8	Emplacement et protection du matériel	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection
7.9	Sécurité des actifs hors des locaux	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection
7.10	Supports de stockage	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection
7.11	Services généraux	#Prévention #Détection	#Disponibilité	#Protection #Détection	#Sécurité_physique	#Protection
7.12	Sécurité du câblage	#Prévention	#Confidentialité #Disponibilité	#Protection	#Sécurité_physique	#Protection
7.13	Maintenance du matériel	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection #Résilience
7.14	Mise au rebut ou recyclage sécurisé(e) du matériel	#Prévention	#Confidentialité	#Protection	#Sécurité_physique #Gestion_des_actifs	#Protection
8.1	Terminaux utilisateurs	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Protection
8.2	Privilèges d'accès	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection
8.3	Restriction d'accès à l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
8.4	Accès au code source	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès #Sécurité_des_applications	#Protection
8.5	Authentification sécurisée	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection
8.6	Dimensionnement	#Prévention #Détection	#Disponibilité	#Identification #Protection #Détection	#Continuité	#Gouvernance_et_écosystème #Protection
8.7	Protection contre les programmes malveillants	#Prévention #Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection #Défense
8.8	Gestion des vulnérabilités techniques	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_menaces_et_des_vulnérabilités	#Gouvernance_et_écosystème #Protection #Défense
8.9	Gestion de la configuration	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Configuration_sécurisée	#Gouvernance_et_écosystème #Protection
8.10	Suppression d'information	#Prévention	#Confidentialité	#Protection	#Protection_des_informations	#Protection
8.11	Masquage des données	#Prévention	#Confidentialité	#Protection	#Protection_des_informations	#Protection
8.12	Prévention de la fuite de données	#Prévention #Détection	#Confidentialité	#Protection #Détection	#Protection_des_informations	#Protection #Défense
8.13	Sauvegarde des informations	#Correction	#Intégrité #Disponibilité	#Récupération	#Continuité	#Protection
8.14	Redondance des moyens de traitement de l'information	#Prévention	#Disponibilité	#Protection	#Continuité #Gestion_des_actifs	#Protection #Résilience
8.15	Journalisation	#Détection	#Confidentialité #Intégrité #Disponibilité	#Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Protection #Défense
8.16	Activités de surveillance	#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
8.17	Synchronisation des horloges	#Détection	#Intégrité	#Protection #Détection	#Gestion_des_événements_de_sécurité_de_l'information	#Protection #Défense
8.18	Utilisation de programmes utilitaires à privilèges	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau #Configuration_sécurisée	#Protection
8.19	Installation de logiciels sur des systèmes en exploitation	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Configuration_sécurisée	#Protection

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
8.20	Mesures liées aux réseaux	#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection
8.21	Sécurité des services en réseau	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.22	Filtrage Internet	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.23	Cloisonnement des réseaux	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.24	Utilisation de la cryptographie	#Prévention	#Confidentialité #Intégrité	#Protection	#Configuration_sécurisée	#Protection
8.25	Cycle de vie de développement sécurisé	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.26	Exigences de sécurité des applications	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection #Défense
8.27	Principes d'ingénierie et d'architecture système sécurisée	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.28	Codage sécurisé	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.29	Tests de sécurité dans le développement et l'acceptation	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Détection	#Sécurité_des_applications #Assurance_de_sécurité_de_l'information #Sécurité_système_et_réseau	#Protection
8.30	Développement externalisé	#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection #Détection	#Sécurité_système_et_réseau #Sécurité_des_applications #Sécurité_des_relations_fournisseurs	#Gouvernance_et_écosystème #Protection
8.31	Séparation des environnements de développement, de test et de production	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
8.32	Gestion des changements	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.33	Informations relatives aux tests	#Prévention	#Confidentialité #Intégrité	#Protection	#Protection_des_informations	#Protection
8.34	Protection des systèmes d'information en cours d'audit et de test	#Prévention	#Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau #Protection_des_informations	#Gouvernance_et_écosystème #Protection

Le Tableau A.2 présente un exemple de création d'une vue par filtrage à l'aide d'une valeur d'attribut particulière ; dans le cas présent #Correction.

Tableau A.2 — Vue de mesures de sécurité #Correction

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.5	Relations avec les autorités	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense #Résilience
5.6	Relations avec des groupes de travail spécialisés	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense
5.24	Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information	#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.26	Réponse aux incidents liés à la sécurité de l'information	#Correction	#Confidentialité #Intégrité #Disponibilité	#Traitement #Récupération	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.28	Recueil de preuves	#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense
5.30	Préparation des TIC pour la continuité d'activité	#Protection #Correction	#Disponibilité	#Protection #Traitement	#Continuité	#Résilience
5.35	Revue indépendante de la sécurité de l'information	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Identification	#Assurance_de_sécurité_de_l'information	#Gouvernance_et_écosystème

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
6.4	Processus disciplinaire	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement	#Sécurité_des_ressources_humaines	#Gouvernance_et_écosystème
8.7	Protection contre les programmes malveillants	#Prévention #Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection #Défense
8.13	Sauvegarde des informations	#Correction	#Intégrité #Disponibilité	#Récupération	#Continuité	#Protection
8.16	Activités de surveillance	#Détection #Correction	#Confidentialité #Intégrité #Disponibilité	#Détection #Traitement	#Gestion_des_événements_de_sécurité_de_l'information	#Défense

A.2 Vues organisationnelles

Il s'agit dans un premier temps de comprendre la raison pour laquelle un attribut spécifique de l'organisation est souhaitable. Par exemple, si une organisation a élaboré ses plans de traitement des risques (voir l'ISO/IEC 27001:2013, 6.1.3 e)) par rapport à des événements, elle peut souhaiter associer un attribut de scénario de risque à chaque mesure du présent document.

Un tel attribut présente l'avantage d'accélérer le processus de traitement de l'ISO/IEC 27001:2013, 6.1.3 c), qui est de comparer les mesures déterminées via le processus de traitement du risque (mesures qualifiées de « nécessaires ») avec celles du présent document pour s'assurer qu'aucune mesure nécessaire n'a été omise.

Une fois que le but et les avantages sont connus, la prochaine étape consiste à déterminer les valeurs d'attribut. Supposons que l'organisation ait identifié 9 événements :

a) perte ou vol d'appareil mobile ;

b) perte ou vol dans les locaux de l'organisation ;

c) force majeure, vandalisme et terrorisme ;

d) défaillance de logiciel, de matériel, d'Internet et des communications ou panne de courant ;

e) fraude ;

f) piratage ;

g) divulgation ;

h) violation de la loi ;

i) ingénierie sociale.

La deuxième étape peut donc consister à affecter un identifiant à chaque événement, par exemple E1, E2, ..., E9.

La troisième étape consiste à copier les identifiants des mesures et les noms de mesures du présent document dans le tableur ou la base de données et d'associer les valeurs d'attributs à chaque mesure. Gardez à l'esprit que chaque mesure peut comporter plusieurs valeurs d'attributs.

La dernière étape consiste à trier la feuille de calcul ou à interroger la base de données pour extraire les informations requises.

Autres exemples d'attributs organisationnels (et de valeurs possibles) :

a) maturité (valeurs de l'ISO/IEC de la série 33000 ou autres modèles de maturité) ;

b) état de mise en œuvre (à faire, en cours, partiellement mis en œuvre, entièrement mis en œuvre) ;

c) priorité (1, 2, 3, etc.) ;

d) secteurs organisationnels concernés (sécurité, TIC, RH, direction générale, etc.) ;

e) événements ;

f) actifs concernés ;

g) développer et exécuter, pour différencier les mesures utilisées dans les différentes étapes du cycle de vie du service ;

h) autres cadres que l'organisation utilise ou depuis lesquels elle pourrait opérer une transition.

Annexe B
(informative)

Correspondance avec l'ISO/IEC 27002:2013

La présente annexe a pour objet de proposer une compatibilité avec la version précédente, l'ISO/IEC 27002:2013, aux organisations qui utilisent actuellement cette norme et souhaitent maintenant passer à l'édition actuelle.

Le Tableau B.1 indique la correspondance des mesures indiquées dans les Articles 5 à 8 avec celles de l'ISO/IEC 27002:2013.

Tableau B.1 — Correspondance entre les mesures du présent document et les mesures de l'ISO/IEC 27002:2013

Identifiant de mesure dans l'ISO/IEC 27002	Identifiant de mesure dans l'ISO/IEC 27002:2013	Nom de la mesure
5.1	05.1.1, 05.1.2	Politiques de sécurité de l'information
5.2	06.1.1	Fonctions et responsabilités liées à la sécurité de l'information
5.3	06.1.2	Séparation des tâches
5.4	07.2.1	Responsabilités de la direction
5.5	06.1.3	Relations avec les autorités
5.6	06.1.4	Relations avec des groupes de travail spécialisés
5.7	Nouveau	Intelligence des menaces
5.8	06.1.5, 14.1.1	Sécurité de l'information dans la gestion de projet
5.9	08.1.1, 08.1.2	Inventaire des informations et des autres actifs associés
5.10	08.1.3, 08.2.3	Utilisation correcte de l'information et des actifs associés
5.11	08.1.4	Restitution des actifs
5.12	08.2.1	Classification de l'information
5.13	08.2.2	Marquage des informations
5.14	13.2.1, 13.2.2, 13.2.3	Transfert de l'information
5.15	09.1.1, 09.1.2	Contrôle d'accès
5.16	09.2.1	Gestion des identités
5.17	09.2.4, 09.3.1, 09.4.3	Informations d'authentification
5.18	09.2.2, 09.2.5, 09.2.6	Droits d'accès
5.19	15.1.1	Sécurité de l'information dans les relations avec les fournisseurs
5.20	15.1.2	Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs

Identifiant de mesure dans l'ISO/IEC 27002	Identifiant de mesure dans l'ISO/IEC 27002:2013	Nom de la mesure
5.21	15.1.3	Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC
5.22	15.2.1, 15.2.2	Suivi, revue et gestion des changements des services fournisseurs
5.23	Nouveau	Sécurité de l'information dans l'utilisation de services en nuage
5.24	16.1.1	Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information
5.25	16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision
5.26	16.1.5	Réponse aux incidents liés à la sécurité de l'information
5.27	16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information
5.28	16.1.7	Recueil de preuves
5.29	17.1.1, 17.1.2, 17.1.3	Sécurité de l'information durant une perturbation
5.30	Nouveau	Préparation des TIC pour la continuité d'activité
5.31	18.1.1, 18.1.5	Identification des exigences légales, statutaires, réglementaires et contractuelles
5.32	18.1.2	Droits de propriété intellectuelle
5.33	18.1.3	Protection des enregistrements
5.34	18.1.4	Vie privée et protection des DCP
5.35	18.2.1	Revue indépendante de la sécurité de l'information
5.36	18.2.2, 18.2.3	Conformité aux politiques et normes de sécurité de l'information
5.37	12.1.1	Procédures d'exploitation documentées
6.1	07.1.1	Présélection
6.2	07.1.2	Conditions générales d'embauche
6.3	07.2.2	Sensibilisation, apprentissage et formation à la sécurité de l'information
6.4	07.2.3	Processus disciplinaire
6.5	07.3.1	Responsabilités consécutivement à la fin ou à la modification du contrat de travail
6.6	13.2.4	Engagements de confidentialité ou de non-divulgation
6.7	06.2.2	Travail à distance
6.8	16.1.2, 16.1.3	Signalement des événements liés à la sécurité de l'information
7.1	11.1.1	Périmètre de sécurité physique
7.2	11.1.2, 11.1.6	Contrôles physiques des accès
7.3	11.1.3	Sécurisation des bureaux, des salles et des équipements
7.4	Nouveau	Surveillance de la sécurité physique

Identifiant de mesure dans l'ISO/IEC 27002	Identifiant de mesure dans l'ISO/IEC 27002:2013	Nom de la mesure
7.5	11.1.4	Protection contre les menaces physiques et environnementales
7.6	11.1.5	Travail dans les zones sécurisées
7.7	11.2.9	Bureau propre et écran vide
7.8	11.2.1	Emplacement et protection du matériel
7.9	11.2.6	Sécurité des actifs hors des locaux
7.10	08.3.1, 08.3.2, 08.3.3	Supports de stockage
7.11	11.2.2	Services généraux
7.12	11.2.3	Sécurité du câblage
7.13	11.2.4	Maintenance du matériel
7.14	11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel
8.1	06.2.1, 11.2.8	Terminaux utilisateurs
8.2	09.2.3	Privilèges d'accès
8.3	09.4.1	Restriction d'accès à l'information
8.4	09.4.5	Accès au code source
8.5	09.4.2	Authentification sécurisée
8.6	12.1.3	Dimensionnement
8.7	12.2.1	Protection contre les programmes malveillants
8.8	12.6.1, 18.2.3	Gestion des vulnérabilités techniques
8.9	Nouveau	Gestion de la configuration
8.10	Nouveau	Suppression d'information
8.11	Nouveau	Masquage des données
8.12	Nouveau	Prévention de la fuite de données
8.13	12.3.1	Sauvegarde des informations
8.14	17.2.1	Redondance des moyens de traitement de l'information
8.15	12.4.1, 12.4.2, 12.4.3	Journalisation
8.16	Nouveau	Activités de surveillance
8.17	12.4.4	Synchronisation des horloges
8.18	09.4.4	Utilisation de programmes utilitaires à privilèges
8.19	12.5.1, 12.6.2	Installation de logiciels sur des systèmes en exploitation
8.20	13.1.1	Mesures liées aux réseaux
8.21	13.1.2	Sécurité des services en réseau
8.22	Nouveau	Filtrage Internet
8.23	13.1.3	Cloisonnement des réseaux

Identifiant de mesure dans l'ISO/IEC 27002	Identifiant de mesure dans l'ISO/IEC 27002:2013	Nom de la mesure
8.24	10.1.1, 10.1.2	Utilisation de la cryptographie
8.25	14.2.1	Cycle de vie de développement sécurisé
8.26	14.1.2, 14.1.3	Exigences de sécurité des applications
8.27	14.2.5	Principes d'ingénierie et d'architecture système sécurisée
8.28	Nouveau	Codage sécurisé
8.29	14.2.8, 14.2.9	Tests de sécurité dans le développement et l'acceptation
8.30	14.2.7	Développement externalisé
8.31	12.1.4, 14.2.6	Séparation des environnements de développement, de test et de production
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestion des changements
8.33	14.3.1	Informations relatives aux tests
8.34	12.7.1	Protection des systèmes d'information en cours d'audit et de test

Le Tableau B.2 indique la correspondance des mesures figurant dans l'ISO/IEC 27002:2013 avec celles du présent document.

Tableau B.2 — Correspondance entre les mesures de l'ISO/IEC 27002:2013 et les mesures du présent document

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
5		Politiques de sécurité de l'information
5.1		Orientations de la direction en matière de sécurité de l'information
5.1.1	5.1	Politiques de sécurité de l'information
5.1.2	5.1	Revue des politiques de sécurité de l'information
6		Organisation de la sécurité de l'information
6.1		Organisation interne
6.1.1	5.2	Fonctions et responsabilités liées à la sécurité de l'information
6.1.2	5.3	Séparation des tâches
6.1.3	5.5	Relations avec les autorités
6.1.4	5.6	Relations avec des groupes de travail spécialisés
6.1.5	5.8	Sécurité de l'information dans la gestion de projet
6.2		Appareils mobiles et télétravail
6.2.1	8.1	Politique en matière d'appareils mobiles
6.2.2	6.7	Télétravail

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
7		Sécurité des ressources humaines
7.1		Avant l'embauche
7.1.1	6.1	Présélection
7.1.2	6.2	Conditions générales d'embauche
7.2		Pendant la durée du contrat
7.2.1	5.4	Responsabilités de la direction
7.2.2	6.3	Sensibilisation, apprentissage et formation à la sécurité de l'information
7.2.3	6.4	Processus disciplinaire
7.3		Rupture, terme ou modification du contrat de travail
7.3.1	6.5	Achèvement ou modification des responsabilités associées au contrat de travail
8		Gestion des actifs
8.1		Responsabilités relatives aux actifs
8.1.1	5.9	Inventaire des actifs
8.1.2	5.9	Propriété des actifs
8.1.3	5.10	Utilisation correcte des actifs
8.1.4	5.11	Restitution des actifs
8.2		Classification de l'information
8.2.1	5.12	Classification de l'information
8.2.2	5.13	Marquage des informations
8.2.3	5.10	Manipulation des actifs
8.3		Manipulation des supports
8.3.1	7.10	Gestion des supports amovibles
8.3.2	7.10	Mise au rebut des supports
8.3.3	7.10	Transfert physique des supports
9		Contrôle d'accès
9.1		Exigences métier en matière de contrôle d'accès
9.1.1	5.15	Politique de contrôle d'accès
9.1.2	5.15	Accès aux réseaux et aux services en réseau
9.2		Gestion de l’accès utilisateur
9.2.1	5.16	Enregistrement et désinscription des utilisateurs
9.2.2	5.18	Maîtrise de la gestion des accès utilisateur
9.2.3	8.2	Gestion des privilèges d’accès

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
9.2.4	5.17	Gestion des informations secrètes d'authentification des utilisateurs
9.2.5	5.18	Revue des droits d'accès utilisateur
9.2.6	5.18	Suppression ou adaptation des droits d'accès
9.3		Responsabilités des utilisateurs
9.3.1	5.17	Utilisation d'informations secrètes d'authentification
9.4		Contrôle de l'accès au système et aux applications
9.4.1	8.3	Restriction d'accès à l'information
9.4.2	8.5	Sécuriser les procédures de connexion
9.4.3	5.17	Système de gestion des mots de passe
9.4.4	8.18	Utilisation de programmes utilitaires à privilèges
9.4.5	8.4	Contrôle d’accès au code source des programmes
10		Cryptographie
10.1		Mesures cryptographiques
10.1.1	8.24	Politique d’utilisation des mesures cryptographiques
10.1.2	8.24	Gestion des clés
11		Sécurité physique et environnementale
11.1		Zones sécurisées
11.1.1	7.1	Périmètre de sécurité physique
11.1.2	7.2	Contrôles physiques des accès
11.1.3	7.3	Sécurisation des bureaux, des salles et des équipements
11.1.4	7.5	Protection contre les menaces extérieures et environnementales
11.1.5	7.6	Travail dans les zones sécurisées
11.1.6	7.2	Zones de livraison et de chargement
11.2		Matériels
11.2.1	7.8	Emplacement et protection du matériel
11.2.2	7.11	Services généraux
11.2.3	7.12	Sécurité du câblage
11.2.4	7.13	Maintenance du matériel
11.2.5	Supprimé	Sortie des actifs
11.2.6	7.9	Sécurité du matériel et des actifs hors des locaux
11.2.7	7.14	Mise au rebut ou recyclage sécurisé(e) du matériel
11.2.8	8.1	Matériel utilisateur laissé sans surveillance

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
11.2.9	7.7	Politique du bureau propre et de l'écran vide
12		Sécurité liée à l'exploitation
12.1		Procédures et responsabilités liées à l'exploitation
12.1.1	5.37	Procédures d'exploitation documentées
12.1.2	8.32	Gestion des changements
12.1.3	8.6	Dimensionnement
12.1.4	8.31	Séparation des environnements de développement, de test et d'exploitation
12.2		Protection contre les programmes malveillants
12.2.1	8.7	Mesures contre les programmes malveillants
12.3		Sauvegarde
12.3.1	8.13	Sauvegarde des informations
12.4		Journalisation et surveillance
12.4.1	8.15	Journalisation des événements
12.4.2	8.15	Protection de l'information journalisée
12.4.3	8.15	Journaux administrateur et opérateur
12.4.4	8.17	Synchronisation des horloges
12.5		Maîtrise des logiciels en exploitation
12.5.1	8.19	Installation de logiciels sur des systèmes en exploitation
12.6		Gestion des vulnérabilités techniques
12.6.1	8.8	Gestion des vulnérabilités techniques
12.6.2	8.19	Restrictions liées à l'installation de logiciels
12.7		Considérations sur l'audit du système d'information
12.7.1	8.34	Mesures relatives à l'audit des systèmes d'information
13		Sécurité des communications
13.1		Installations de management de la sécurité des réseaux
13.1.1	8.20	Mesures liées aux réseaux
13.1.2	8.21	Sécurité des services en réseau
13.1.3	8.23	Cloisonnement des réseaux
13.2		Transfert de l'information
13.2.1	5.14	Politiques et procédures de transfert de l'information
13.2.2	5.14	Accords en matière de transfert d'information
13.2.3	5.14	Messagerie électronique

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
13.2.4	6.6	Engagements de confidentialité ou de non-divulgation
14		Acquisition, développement et maintenance des systèmes d'information
14.1		Exigences de sécurité applicables aux systèmes d'information
14.1.1	5.8	Analyse et spécification des exigences de sécurité de l'information
14.1.2	8.26	Sécurisation des services d'application sur les réseaux publics
14.1.3	8.26	Protection des transactions liées aux services d'application
14.2		Sécurité des processus de développement et d'assistance technique
14.2.1	8.25	Politique de développement sécurisé
14.2.2	8.32	Procédures de contrôle des changements apportés au système
14.2.3	8.32	Revue technique des applications après changement apporté à la plateforme d'exploitation
14.2.4	8.32	Restrictions relatives aux changements apportés aux progiciels
14.2.5	8.27	Principes d'ingénierie de la sécurité des systèmes
14.2.6	8.31	Environnement de développement sécurisé
14.2.7	8.30	Développement externalisé
14.2.8	8.29	Phase de test de la sécurité du système
14.2.9	8.29	Test de conformité du système
14.3		Données de test
14.3.1	8.33	Protection des données de test
15		Relations avec les fournisseurs
15.1		Sécurité de l'information dans les relations avec les fournisseurs
15.1.1	5.19	Politique de sécurité de l'information dans les relations avec les fournisseurs
15.1.2	5.20	La sécurité dans les accords conclus avec les fournisseurs
15.1.3	5.21	Chaîne d'approvisionnement informatique
15.2		Gestion de la prestation du service
15.2.1	5.22	Surveillance et revue des services des fournisseurs
15.2.2	5.22	Gestion des changements apportés dans les services des fournisseurs
16		Gestion des incidents liés à la sécurité de l'information
16.1		Gestion des incidents liés à la sécurité de l'information et améliorations
16.1.1	5.24	Responsabilités et procédures
16.1.2	6.8	Signalement des événements liés à la sécurité de l'information
16.1.3	6.8	Signalement des failles liées à la sécurité de l'information

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
16.1.4	5.25	Appréciation des événements liés à la sécurité de l'information et prise de décision
16.1.5	5.26	Réponse aux incidents liés à la sécurité de l'information
16.1.6	5.27	Tirer des enseignements des incidents liés à la sécurité de l'information
16.1.7	5.28	Recueil de preuves
17		Aspects de la sécurité de l'information dans la gestion de la continuité d'activité
17.1		Continuité de la sécurité de l'information
17.1.1	5.29	Organisation de la continuité de la sécurité de l'information
17.1.2	5.29	Mise en œuvre de la continuité de la sécurité de l'information
17.1.3	5.29	Vérifier, revoir et évaluer la continuité de la sécurité de l'information
17.2		Redondances
17.2.1	8.14	Disponibilité des moyens de traitement de l'information
18		Conformité
18.1		Conformité aux obligations légales et réglementaires
18.1.1	5.31	Identification de la législation et des exigences contractuelles applicables
18.1.2	5.32	Droits de propriété intellectuelle
18.1.3	5.33	Protection des enregistrements
18.1.4	5.34	Protection de la vie privée et protection des données à caractère personnel
18.1.5	5.31	Réglementation relative aux mesures cryptographiques
18.2		Revue de la sécurité de l'information
18.2.1	5.35	Revue indépendante de la sécurité de l'information
18.2.2	5.36	Conformité aux politiques et normes de sécurité
18.2.3	5.36, 8.8	Examen de la conformité technique

Bibliographie

Normes ISO/IEC

[1] ISO 9000, *Systèmes de management de la qualité — Principes essentiels et vocabulaire*

[2] ISO/IEC 11770 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Gestion de clés*

[3] ISO/IEC 15408 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI*

[4] ISO 15489 (toutes les parties), *Information et documentation — Gestion des documents d'activité*

[5] ISO/IEC 17788:2014, *Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire*

[6] ISO/IEC 17789, *Technologies de l'information — Informatique en nuage — Architecture de référence*

[7] ISO/IEC 19086 (toutes les parties), *Informatique en nuage — Cadre de travail de l'accord du niveau de service*

[8] ISO/IEC 19770 (toutes les parties), *Technologies de l'information — Gestion de biens de logiciel*

[9] ISO/IEC 19941, *Technologies de l'information — Informatique en nuage — Interopérabilité et portabilité*

[10] ISO/IEC 20889, *Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée*

[11] ISO 21500, *Lignes directrices sur le management de projet*

[12] ISO 22301, *Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences*

[13] ISO 22313, *Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301*

[14] ISO/TS 22317, *Sécurité sociétale — Systèmes de management de la continuité en affaires — Lignes directrices pour l'analyse d'impact sur l'activité*

[15] ISO 22396, *Sécurité et résilience — Résilience des communautés — Lignes directrices pour l'échange d'informations entre les organismes*

[16] ISO/IEC/TS 23167, *Information technology — Cloud computing — Common technologies and techniques*

[17] ISO/IEC 23751,[1] *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*

[18] ISO/IEC 24760 (toutes les parties), *Sécurité IT et confidentialité — Cadre pour la gestion de l'identité*

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

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

[21] ISO/IEC 27007, *Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*

[22] ISO/IEC/TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[23] ISO/IEC 27011, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications*

[24] ISO/IEC/TR 27016, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Économie organisationnelle*

[25] ISO/IEC 27017, *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*

[26] ISO/IEC 27018, *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

[27] ISO/IEC 27019, *Technologies de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie*

[28] ISO/IEC 27031, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité*

[29] ISO/IEC 27033 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Sécurité de réseau*

[30] ISO/IEC 27034 (toutes les parties), *Technologies de l'information — Sécurité des applications*

[31] ISO/IEC 27035 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information*

[1] En cours d'élaboration

[32] ISO/IEC 27036 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur*

[33] ISO/IEC 27037, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques*

[34] ISO/IEC 27040, *Technologies de l'information — Techniques de sécurité — Sécurité de stockage*

[35] ISO/IEC 27050 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Découverte électronique*

[36] ISO/IEC/TS 27101, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*

[37] ISO/IEC 27701, *Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

[38] ISO 27799, *Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002*

[39] ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé*

[40] ISO/IEC 29115, *Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité*

[41] ISO/IEC 29134, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée*

[42] ISO/IEC 29146, *Technologies de l'information — Techniques de sécurité — Cadre pour gestion d'accès*

[43] ISO/IEC 29147, *Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité*

[44] ISO 30000, *Navires et technologie maritime — Systèmes de management de recyclage des navires — Spécifications relatives aux systèmes de management pour les chantiers de recyclage des navires, sûrs et non polluants*

[45] ISO/IEC 30111, *Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité*

[46] ISO 31000:2018, *Management du risque — Lignes directrices*

[47] IEC 31010:2019, *Management du risque — Techniques d'appréciation du risque*

Références à la littérature

[48] INFORMATION SECURITY FORUM (ISF). Standard of Good Practice for Information Security 2018 de l'ISF, août 2018. Disponible à l'adresse https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

[49] ITIL® Foundation, ITIL 4 edition, AXELOS, février 2019, ISBN : 9780113316076

[50] National Institute of Standards and Technology (NIST), SP 800-53B, Control Baselines for Information Systems and Organizations, Révision 5 (Projet) [en ligne]. Juillet 2020 [consulté le 2020-07-31]. Disponible à l'adresse https://doi.org/10.6028/NIST.SP.800-53B-draft

[51] National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Révision 2 [en ligne]. Décembre 2018 [consulté le 2020-07-31]. Disponible à l'adresse https://doi.org/10.6028/NIST.SP.800-37r2

[52] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks [en ligne], 2017 [consulté le 2020-07-31]. Disponible à l'adresse https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

[53] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [en ligne] [consulté le 2020-10-22]. Disponible à l'adresse https://github.com/OWASP/DevGuide

[54] National Institute of Standards and Technology (NIST). SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management [en ligne]. Février 2020 [consulté le 2020-07-31]. Disponible à l'adresse https://doi.org/10.6028/NIST.SP.800-63b

[55] OASIS. Structured Threat Information Expression [en ligne]. Disponible à l'adresse https://www.oasis-open.org/standards#stix2.0

[56] OASIS. Trusted Automated Exchange of Indicator Information [en ligne]. Disponible à l'adresse https://www.oasis-open.org/standards#taxii2.0