Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1603

(03/2018)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'informatique en nuage – Conception de la sécurité de l'informatique en nuage

Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage

Recommandation UIT-T X.1603

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	**X.1602–X.1639**
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1603

Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage

Résumé

La Recommandation UIT-T X.1603 analyse les exigences de sécurité des données pour le service de surveillance de l'informatique en nuage et traite notamment des exigences relatives à la portée des données de surveillance, du cycle de vie des données de surveillance, des exigences de sécurité concernant l'acquisition des données de surveillance et des exigences de sécurité concernant le stockage des données de surveillance. S'agissant des exigences relatives à la portée des données de surveillance, il est question de l'étendue de la surveillance nécessaire que les fournisseurs de services en nuage (CSP) devraient assurer pour garantir la sécurité de l'informatique en nuage ainsi que de la plus grande étendue possible de la surveillance assurée par les fournisseurs CSP. Le cycle de vie des données de surveillance inclut la création, le stockage, l'utilisation, la migration, la présentation, la destruction et la sauvegarde des données. Pour l'acquisition des données de surveillance, on détermine les exigences de sécurité concernant les techniques d'acquisition d'un service de surveillance. Pour le stockage des données de surveillance, on détermine les exigences de sécurité applicables aux fournisseurs CSP pour le stockage des données de surveillance.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1603	29-03-2018	17	11.1002/1000/13406

Mots clés

Nuage, sécurité des données, surveillance.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

© UIT 2018

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	3
4	Abréviations et acronymes	4
5	Conventions	4
6	Présentation générale	5
7	Portée des données de surveillance pour l'informatique en nuage	5
8	Cycle de vie des données de surveillance dans l'informatique en nuage	6
	8.1 Collecte de données de surveillance	6
	8.2 Stockage des données de surveillance	6
	8.3 Utilisation des données de surveillance	7
	8.4 Migration des données de surveillance	7
	8.5 Analyse des données de surveillance	7
	8.6 Présentation des données de surveillance	7
	8.7 Destruction des données de surveillance	7
	8.8 Sauvegarde des données de surveillance	7
9	Menaces et problèmes de sécurité pour les données de surveillance de l'informatique en nuage	7
	9.1 Menaces et problèmes de sécurité à l'étape de la collecte de données de surveillance	8
	9.2 Menaces et problèmes de sécurité à l'étape du stockage des données de surveillance	8
	9.3 Menaces et problèmes de sécurité à l'étape de l'utilisation des données de surveillance	9
	9.4 Menaces et problèmes de sécurité à l'étape de la migration des données de surveillance	9
	9.5 Menaces et problèmes de sécurité à l'étape de l'analyse des données de surveillance	9
	9.6 Menaces et problèmes de sécurité à l'étape de la présentation des données de surveillance	9
	9.7 Menaces et problèmes de sécurité à l'étape de la destruction des données de surveillance	9
	9.8 Menaces et problèmes de sécurité à l'étape de la sauvegarde des données de surveillance	10
10	Exigences de sécurité pour les données de surveillance de l'informatique en nuage	10
	10.1 Exigences de sécurité pour la collecte des données de surveillance	10
	10.2 Exigences de sécurité pour le stockage des données de surveillance	11

Page

10.3 Exigences de sécurité pour l'utilisation des données de surveillance 11
10.4 Exigences de sécurité pour la migration des données de surveillance 12
10.5 Exigences de sécurité pour l'analyse des données de surveillance 12
10.6 Exigences de sécurité pour la présentation des données de surveillance 12
10.7 Exigences de sécurité pour la destruction des données de surveillance 13
10.8 Exigences de sécurité pour la sauvegarde des données de surveillance 13
Bibliographie 15

Recommandation UIT-T X.1603

Exigences de sécurité des données pour le service de surveillance de l'informatique en nuage

1 Domaine d'application

La présente Recommandation vise à définir les exigences de sécurité des données pour le service de surveillance de l'informatique en nuage. Elle vise à analyser les menaces et les problèmes de sécurité des données liés au service de surveillance dans un environnement d'informatique en nuage et à décrire les exigences de sécurité des données pour le service de surveillance, notamment en ce qui concerne la portée des données, le cycle de vie des données, l'acquisition de données et le stockage des données. La présente Recommandation peut être utilisée par les fournisseurs de services en nuage (CSP) qui fournissent des services de surveillance aux clients de services en nuage (CSC).

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-NIST-SP-800-53]: vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif souvent indispensable pour pouvoir accéder aux ressources d'un système d'information.

3.1.2 capacité [b-ISO/CEI 19440]: qualité permettant d'accomplir une activité donnée.

3.1.3 informatique en nuage [b-UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre service.

NOTE – Comme exemples de ressources, on peut citer les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et les équipements de stockage.

3.1.4 service en nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes par l'intermédiaire de l'informatique en nuage (voir le paragraphe 3.1.3) demandées à l'aide d'une interface définie.

3.1.5 client de services en nuage [b-UIT-T Y.3500]: partie (voir le paragraphe 3.1.15) à une relation commerciale aux fins de l'utilisation de services en nuage (voir le paragraphe 3.1.4).

NOTE – Une relation commerciale n'implique pas nécessairement des accords financiers.

3.1.6 partenaire de services en nuage [b-UIT-T Y.3500]: partie (voir le paragraphe 3.1.15) fournissant un appui ou une aide aux activités d'un fournisseur de services en nuage (voir le paragraphe 3.1.7), d'un client de services en nuage (voir le paragraphe 3.1.5), ou des deux.

3.1.7 fournisseur de services en nuage [b-UIT-T Y.3500]: partie (voir le paragraphe 3.1.15) qui met à disposition des services en nuage (voir le paragraphe 3.1.4).

3.1.8 utilisateur de services en nuage [b-UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services en nuage (voir le paragraphe 3.1.5) qui utilise des services en nuage (voir le paragraphe 3.1.4).

NOTE – Comme exemples de ces entités, on peut citer les dispositifs et applications.

3.1.9 communications en tant que service (CaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client du service en nuage (voir le paragraphe 3.1.5) est une interaction et une collaboration en temps réel.

NOTE – La communication CaaS peut correspondre à la fourniture de capacités de plate-forme et de capacités d'application.

3.1.10 nuage communautaire [b-UIT-T Y.3500]: modèle de déploiement d'un nuage dans lequel les services en nuage (voir le paragraphe 3.1.4) prennent en charge exclusivement un ensemble défini de clients de services en nuage (voir le paragraphe 3.1.5) et sont utilisées en partage par ce même ensemble de clients, qui ont des exigences communes et une relation entre eux, les ressources étant contrôlées par au moins un membre de cet ensemble.

3.1.11 hyperviseur [b-NIST-SP-800-125]: élément de virtualisation qui gère les systèmes d'exploitation invités sur un serveur et contrôle le flux d'instructions entre ces systèmes d'exploitation et le matériel physique.

3.1.12 infrastructure en tant que service (IaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité de nuage fourni au client de services en nuage (voir le paragraphe 3.1.5) correspond à des capacités d'infrastructure.

NOTE – Le client de services en nuage (voir le paragraphe 3.1.5) ne gère pas ni ne contrôle les ressources physiques et virtuelles sous-jacentes, mais contrôle les systèmes d'exploitation, le stockage et les applications déployées qui utilisent les ressources physiques et virtuelles. Le client de services en nuage (voir le paragraphe 3.1.5) peut en outre avoir une capacité limitée de contrôler certains éléments du réseau (par exemple, pare-feux du serveur).

3.1.13 multilocataires [b-UIT-T Y.3500]: attribution de ressources physiques ou virtuelles selon laquelle plusieurs locataires (voir le paragraphe 3.1.24) ainsi que leurs calculs et leurs données sont isolés les uns des autres et inaccessibles entre eux.

3.1.14 réseau en tant que service (NaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client de services en nuage (voir le paragraphe 3.1.5) correspond à des capacités de connectivité de transport et à des capacités de réseau connexes.

NOTE – Le réseau NaaS peut fournir l'un quelconque des trois types de capacités de nuage.

3.1.15 partie [b-ISO/CEI 27729]: personne physique ou morale, constituée ou non en société, ou groupe de l'une ou l'autre de ces personnes.

3.1.16 information d'identification personnelle [b-ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte, ou b) est ou peut être directement ou indirectement liée à une personne.

3.1.17 plate-forme en tant que service (PaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité de nuage fourni au client du service en nuage (voir le paragraphe 3.1.5) correspond à des capacités de plate-forme.

3.1.18 nuage privé [b-UIT-T Y.3500]: modèle de déploiement du nuage où les services en nuage (voir le paragraphe 3.1.4) sont utilisés exclusivement par un seul client de services en nuage (voir le paragraphe 3.1.5) et où les ressources sont contrôlées par le client de services en nuage (voir le paragraphe 3.1.5).

3.1.19 nuage public [b-UIT-T Y.3500]: modèle de déploiement du nuage où les services en nuage (voir le paragraphe 3.1.4) peuvent être mis à la disposition de tout client de services en nuage (voir le paragraphe 3.1.5) et où les ressources sont contrôlées par le fournisseur de services en nuage (voir le paragraphe 3.1.7).

3.1.20 domaine de sécurité [b-UIT-T X.810]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est assujetti à la politique de sécurité pour les activités indiquées et la politique de sécurité est administrée par l'autorité de sécurité pour le domaine de sécurité.

3.1.21 atteinte à la sécurité [b-UIT-T E.409]: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

3.1.22 accord de niveau de service (SLA) [b-ISO/CEI 20000-1]: accord écrit entre le prestataire de service et le client qui identifie les services et les objectifs de service.

NOTE 1 – Un accord de niveau de service peut également être conclu entre le prestataire de service et un fournisseur, un groupe interne ou un client agissant en qualité de fournisseur.

NOTE 2 – Un accord de niveau de service peut être intégré dans un contrat ou dans un autre type d'accord écrit.

3.1.23 logiciel en tant que service (SaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité en nuage fourni au client de services en nuage (voir le paragraphe 3.1.5) correspond à des capacités d'application.

3.1.24 locataire [b-UIT-T Y.3500]: un ou plusieurs utilisateurs de services en nuage (voir le paragraphe 3.1.8) utilisant en partage l'accès à un ensemble de ressources physiques et virtuelles.

3.1.25 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, susceptible de nuire à un système ou à une organisation.

3.1.26 vulnérabilité [b-NIST-SP-800-30]: faille dans un système d'information, les procédures de sécurité système, les contrôles internes ou la mise en œuvre, qui pourrait être exploitée par une source de menace.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 données de surveillance: les données de surveillance sont les données de sortie du service de surveillance du nuage, qui aident les fournisseurs CSP et les clients CSC à gérer les plates-formes et les ressources en nuage.

3.2.2 service de surveillance: l'activité du service de surveillance consiste à surveiller la qualité de service fournie au regard des niveaux de service définis dans l'accord de niveau de service (SLA) entre le client de services en nuage et le fournisseur de services en nuage.

3.2.3 données de surveillance nécessaires: les données de surveillance nécessaires sont utilisées pour maintenir les niveaux de service agréés. Elles peuvent aider le fournisseur CSP à assurer la sécurité et la stabilité des plates-formes d'informatique en nuage. Ces données peuvent être notamment (la liste n'est pas exhaustive) des données de surveillance sur le système de gestion, des données de surveillance sur les ressources physiques, des données de surveillance sur le réseau, etc. Les données de surveillance nécessaires sont principalement utilisées par les fournisseurs CSP, mais peuvent également être communiquées aux clients CSC.

3.2.4 données de surveillance facultatives: les données de surveillance facultatives sont communiquées à la demande des clients CSC afin de fournir un service de surveillance du nuage. Ces données peuvent être notamment (la liste n'est pas exhaustive) des données de surveillance sur les machines virtuelles, des données de surveillance sur le service de stockage des données, des données de surveillance sur les applications des clients CSC sur le nuage, etc.

3.2.5 machine virtuelle (VM): reproduction efficace, isolée et logique d'une machine réelle.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

BCP plan de continuité des activités (*business continuity plan*)

CaaS communication en tant que service (*communications as a service*)

CPU unité centrale de traitement (*central processing unit*)

CSC client de services en nuage (*cloud service customer)*

CSN partenaire de services en nuage (*cloud service partner*)

CSP fournisseur de services en nuage (*cloud service provider*)

CSU utilisateur de services en nuage (*cloud service user*)

DDOS déni de service réparti (*distributed denial of service*)

DNS système des noms de domaine *(domain name system*)

DOS déni de service (*denial of service*)

IaaS infrastructure en tant que service *(infrastructure as a service*)

IAM gestion des identités et de l'accès (*identity and access management*)

IP protocole Internet (*Internet protocol*)

IT technologies de l'information, informatique (*information technology*)

NaaS réseau en tant que service (*network as a service*)

OS système d'exploitation (*operating system*)

PaaS plate-forme en tant que service (*platform as a service*)

PII information d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

SaaS logiciel en tant que service (*software as a service*)

SIM module d'identification de l'abonné (*subscriber identity module*)

SLA accord de niveau de service (*service level agreement*)

TIC technologies de l'information et de la communication

VM machine virtuelle (*virtual machine*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

6 Présentation générale

La présente Recommandation vise à analyser les exigences de sécurité des données pour le service de surveillance de l'informatique en nuage, notamment en ce qui concerne la portée des données de surveillance, le cycle de vie des données des données de surveillance, les menaces et les problèmes de sécurité et les exigences de sécurité des données de surveillance pour l'informatique en nuage.

La section consacrée à la portée des données de surveillance décrit deux types de données de surveillance pour l'informatique en nuage, à savoir les données nécessaires et les données facultatives, et présente des cas d'utilisation.

Les sections concernant le cycle de vie des données de surveillance et les menaces et les problèmes de sécurité décrivent les étapes du cycle de vie et les menaces et les problèmes de sécurité aux étapes de la collecte, du stockage, de l'utilisation, de la migration, de l'analyse, de la présentation, de la destruction et de la sauvegarde des données de surveillance de l'informatique en nuage.

La section consacrée aux exigences de sécurité des données de surveillance décrit les exigences détaillées applicables à chaque étape du cycle de vie des données de surveillance de l'informatique en nuage.

7 Portée des données de surveillance pour l'informatique en nuage

Dans un environnement d'informatique en nuage, il existe deux types de données de surveillance: les données de surveillance nécessaires et les données de surveillance facultatives.

Les données de surveillance nécessaires sont utilisées pour maintenir le niveau de service agréé (SLA). Elles peuvent aider le fournisseur CSP à exploiter la plate-forme d'informatique en nuage de façon stable et sécurisée. Ces données peuvent être notamment (la liste n'est pas exhaustive) des données de surveillance sur le système de gestion, des données de surveillance sur les ressources physiques et des données de surveillance sur le réseau. Les données de surveillance nécessaires sont principalement utilisées par les fournisseurs CSP, mais peuvent également être communiquées aux clients CSC.

Les données de surveillance facultatives sont communiquées à la demande du client CSC en vue de la fourniture du service de surveillance par le fournisseur CSP. Ces données peuvent être notamment (la liste n'est pas exhaustive) des données de surveillance sur les machines virtuelles, des données de surveillance sur le service de stockage des données et des données associées à la surveillance des applications du client CSC sur le nuage.

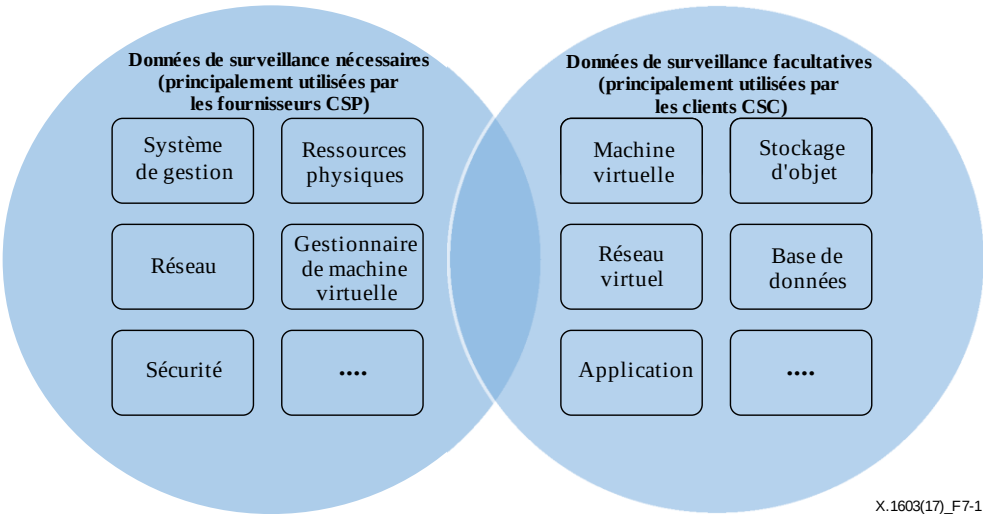

Figure 7-1 – Cas d'utilisation des deux types de données de surveillance

Les données de surveillance nécessaires sont principalement utilisées par les fournisseurs CSP, mais peuvent également être utilisées par les clients CSC. A titre d'exemple, les données de surveillance sur les ressources physiques du nuage, principalement utilisées par les fournisseurs CSP pour maintenir la stabilité de la plate-forme d'informatique en nuage, peuvent aussi être utilisées par les clients CSC lorsque les ressources physiques liées à l'informatique en nuage leur sont fournies en tant que service.

Les données de surveillance facultatives sont fournies à la demande des clients CSC, et sont principalement utilisées par ceux-ci. Les fournisseurs CSP peuvent également utiliser ces données pour maintenir le niveau de service agréé. A titre d'exemple, les clients CSC peuvent solliciter des données liées à la surveillance de leurs propres applications sur le nuage. Ces données sont alors fournies par le fournisseur CSP et sont utilisées par les clients CSC pour mieux gérer leurs applications sur le nuage. Un fournisseur CSP peut, par exemple, utiliser les données de surveillance d'une base de données en tant que service (DBaaS) pour assurer la sécurité et la stabilité des ressources de la base de données et du service en nuage.

La relation entre ces deux types de données de surveillance est illustrée dans la Figure 7-1.

8 Cycle de vie des données de surveillance dans l'informatique en nuage

Cette section décrit le cycle de vie des données de surveillance dans l'informatique en nuage et met en évidence les principales différences entre le cycle de vie de ces données et le cycle de vie d'autres données dans l'informatique en nuage.

8.1 Collecte de données de surveillance

La collecte de données de surveillance découle de l'acquisition de données de surveillance et de la transmission de ces données vers un serveur de stockage. La majorité des données de surveillance sont créées dans le cadre de l'utilisation du service en nuage par le client CSC. Des données de surveillance nécessaires peuvent également être créées dans le cadre d'autres activités de surveillance du service en nuage.

8.2 Stockage des données de surveillance

Une fois que des données de surveillance ont été collectées, elles peuvent être stockées localement dans les ressources en nuage du client CSC ou dans les serveurs de stockage des données de surveillance du fournisseur CSP.

8.3 Utilisation des données de surveillance

Les données de surveillance peuvent être utilisées par le fournisseur CSP pour assurer la qualité de fonctionnement et la sécurité de la plate-forme en nuage et du service en nuage; elles peuvent également être utilisées par les clients CSC pour assurer la qualité de fonctionnement et la sécurité des ressources en nuage.

8.4 Migration des données de surveillance

Lors de la migration des ressources en nuage, il est possible de faire migrer les données de surveillance conjointement avec ces ressources.

8.5 Analyse des données de surveillance

Les données de surveillance peuvent être analysées par le fournisseur CSP et par le client CSC pour connaître l'état des ressources de la plate-forme en nuage, afin de mieux les gérer et les sécuriser.

8.6 Présentation des données de surveillance

Il est recommandé que les données de surveillance soient présentées de façon adéquate, afin qu'elles puissent favoriser une meilleure gestion du niveau de service agréé et de la sécurité du nuage. Etant donné que le volume de données de surveillance de l'informatique en nuage peut être considérable, il est recommandé que ces données soient résumées de telle sorte qu'elles soient intelligibles et manipulables.

8.7 Destruction des données de surveillance

Afin de garantir la sécurité des données de surveillance, le fournisseur CSP est tenu de détruire ces données lorsque les clients CSC en font la demande.

Les fournisseurs CSP peuvent, à titre d'option, détruire les données de surveillance au bout d'un certain temps à compter de la création de ces données.

8.8 Sauvegarde des données de surveillance

Il est obligatoire de créer des sauvegardes des données de surveillance et de restaurer les données à partir des sauvegardes.

9 Menaces et problèmes de sécurité pour les données de surveillance de l'informatique en nuage

Les paragraphes 7 et 8 de la Recommandation [b-UIT-T X.1601] présentent les menaces et les problèmes de sécurité visant les fournisseurs CSP et les clients CSC dans le domaine de l'informatique en nuage; les données de surveillance de l'informatique en nuage sont exposées à des menaces et problèmes de sécurité analogues, qui sont également définis dans la Recommandation [b-UIT-T X.1601]. Certaines de ces menaces et certains de ces problèmes de sécurité sont présentés ci-après (la liste n'est pas exhaustive:

a) perte et fuite de données;

b) accès non sécurisé aux services;

c) accès non autorisé aux fonctions d'administration;

d) menaces internes;

e) perte de confiance;

f) perte de gouvernance;

g) perte de confidentialité;

h) indisponibilité des services;

i) détournement de la propriété intellectuelle;

j) environnement partagé;

k) conflit juridictionnel;

l) migration et intégration médiocres.

A chaque étape de leur cycle de vie, les données de surveillance de l'informatique en nuage sont exposées à certaines menaces et à certains problèmes de sécurité.

9.1 Menaces et problèmes de sécurité à l'étape de la collecte de données de surveillance

a) collecte de données sans autorisation: un fournisseur CSP ou des auteurs d'attaques peuvent collecter les données de surveillance d'un client CSC sans permission ni autorisation.

b) vulnérabilité de l'interface d'acquisition: des auteurs d'attaques peuvent exploiter une vulnérabilité de l'interface d'acquisition des données de surveillance.

c) usurpation d'identité: des auteurs d'attaques peuvent se substituer au système de gestion ou au serveur de stockage des données du service de surveillance du nuage et provoquer la perte de données de surveillance.

d) interception et falsification: des auteurs d'attaques peuvent utiliser des attaques par intercepteur ou d'autres attaques sur le réseau pour falsifier ou intercepter des données de surveillance.

e) accès non sécurisé aux services: à l'étape de la collecte des données de surveillance, l'accès non sécurisé aux interfaces de collecte de données peut entraîner la perte de données de surveillance.

f) accès non autorisé aux fonctions d'administration: l'accès non autorisé aux fonctions d'administration du système de collecte de données de surveillance du fournisseur CSP ou du système du client CSC peut entraîner la perte de données de surveillance. Un auteur d'attaque peut, par exemple, exploiter une vulnérabilité du système pour obtenir un accès non autorisé aux fonctions d'administration du système du client CSC et remplacer l'adresse IP de destination de la collecte des données de surveillance par sa propre adresse IP.

9.2 Menaces et problèmes de sécurité à l'étape du stockage des données de surveillance

a) perte et fuite de données: étant donné que l'environnement des services en nuage est, en règle générale, un environnement multilocataires, la perte ou la fuite de données représente une grave menace tant pour le client CSC et que pour le fournisseur CSP. L'absence de gestion appropriée des informations cryptographiques, comme les clés de chiffrement, les codes d'authentification et le privilège d'accès, pourrait entraîner des préjudices considérables, tels que la perte de données ou une fuite inattendue de données vers l'extérieur. Par exemple, l'insuffisance des contrôles d'authentification, d'autorisation et de vérification, la mauvaise utilisation des clés de chiffrement et/ou d'authentification, les défaillances opérationnelles, les problèmes de destruction des données, les questions de juridiction et de politique, la fiabilité des centres de données et le rétablissement après une catastrophe sont reconnus comme étant les principales menaces.

b) indisponibilité des services: un serveur de stockage des données de surveillance peut être visé par une attaque par déni de service (DoS) ou par déni de service réparti (DDoS); de plus, ces attaques peuvent entraîner une défaillance du matériel de stockage des données de surveillance et, de ce fait, la perte ou la destruction de données.

9.3 Menaces et problèmes de sécurité à l'étape de l'utilisation des données de surveillance

a) utilisation abusive des données: les données de surveillance du client CSC peuvent être utilisées de façon abusive par le fournisseur CSP. Elles peuvent être utilisées par le fournisseur CSP afin de maintenir le niveau de service agréé et d'assurer le fonctionnement de la plate-forme et des ressources d'informatique en nuage, mais elles peuvent également être utilisées à d'autres fins par le fournisseur CSP, sans la permission du client CSC.

b) menaces internes: un employé du fournisseur CSP ou du client CSC peut utiliser de façon abusive les données de surveillance du client CSC, à d'autres fins que celles prévues.

c) vulnérabilité du système: des données de surveillance peuvent être perdues lors de leur utilisation, en raison de vulnérabilités du système.

d) écoutes illicites: les données de surveillance peuvent faire l'objet d'écoutes illicites de la part des auteurs d'attaques.

9.4 Menaces et problèmes de sécurité à l'étape de la migration des données de surveillance

a) utilisation abusive des données: les données de surveillance peuvent être déplacées entre différents emplacements physiques. Il est primordial de prendre des mesures pour prévenir l'utilisation abusive des données lors de la transmission des données de surveillance vers différents emplacements.

b) usurpation d'identité: des auteurs d'attaques peuvent se substituer au système de gestion ou au serveur de stockage des données du service de surveillance du nuage et provoquer la perte ou l'utilisation abusive de données de surveillance.

c) interception et falsification: des auteurs d'attaques peuvent utiliser des attaques par intercepteur ou d'autres attaques sur le réseau pour falsifier ou intercepter des données de surveillance.

9.5 Menaces et problèmes de sécurité à l'étape de l'analyse des données de surveillance

a) utilisation abusive des données: les données de surveillance du client CSC peuvent être utilisées de façon abusive par le fournisseur CSP lors de l'analyse des données.

b) vulnérabilité du système: des données de surveillance peuvent être perdues en raison d'une vulnérabilité du système d'analyse des données.

c) attaque par déni de service: un serveur d'analyse des données de surveillance peut être visé par une attaque DoS ou DDoS.

9.6 Menaces et problèmes de sécurité à l'étape de la présentation des données de surveillance

a) utilisation abusive des données: les données de surveillance du client CSC peuvent être utilisées de façon abusive (ou présentées sans la permission du client CSC) par le fournisseur CSP lors de la présentation des données.

b) vulnérabilité du système: des données de rapports et des données d'analyse peuvent être perdues en raison d'une vulnérabilité du système de présentation des données.

c) représentation erronée: les données de surveillance du client CSC peuvent être représentées de façon erronée lors de la présentation des données.

9.7 Menaces et problèmes de sécurité à l'étape de la destruction des données de surveillance

a) usurpation d'identité: des auteurs d'attaques peuvent se substituer au système de gestion du service de surveillance du nuage et provoquer la perte d'autres données de surveillance.

b) vulnérabilité du système d'exploitation: des données de surveillance peuvent être perdues lors de leur utilisation, en raison d'une vulnérabilité du système.

9.8 Menaces et problèmes de sécurité à l'étape de la sauvegarde des données de surveillance

a) vulnérabilité du système d'exploitation: des données de surveillance peuvent être perdues lors de leur sauvegarde, entraînant l'impossibilité de restaurer les données, en raison d'une vulnérabilité du système.

10 Exigences de sécurité pour les données de surveillance de l'informatique en nuage

Cette section identifie les exigences de sécurité des données pour le service de surveillance de l'informatique en nuage.

10.1 Exigences de sécurité pour la collecte des données de surveillance

Les exigences de sécurité pour la collecte de données de surveillance sont les suivantes:

a) il est obligatoire que les données de surveillance facultatives soient créées uniquement à la demande du client CSC;

b) il est recommandé d'envoyer une notification au client CSC lorsque des données de surveillance nécessaires sont créées;

c) il est recommandé d'informer le client CSC de la portée des données de surveillance;

d) il est obligatoire de préserver l'intégrité et l'exactitude des données de surveillance;

e) il est recommandé d'utiliser des techniques d'acquisition des données classiques;

f) il est recommandé de disposer de méthodes de contrôle d'accès aux interfaces d'acquisition des données de surveillance, par exemple, d'une liste blanche, d'une liste noire, etc.;

g) il est recommandé de disposer de méthodes cryptographiques pour garantir la sécurité de l'interface d'acquisition des données de surveillance;

h) il est recommandé d'utiliser des protocoles réseau classiques entre les ressources en nuage et les serveurs de stockage des données de surveillance.

Le Tableau 10-1 fournit un résumé mettant en correspondance les menaces de sécurité liées à la collecte de données de surveillance et les exigences de sécurité.

Tableau 10-1 – Collecte de données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Collecte de données sans autorisation	a), b), c)
Vulnérabilité de l'interface d'acquisition	d), e), f), g)
Usurpation d'identité	d), e), f), g), h)
Interception et falsification	h)
Accès non sécurisé aux services	b), d), e), f), g), h)
Accès non autorisé aux fonctions d'administration	d), e), f), g), h)

10.2 Exigences de sécurité pour le stockage des données de surveillance

Les exigences de sécurité pour le stockage des données de surveillance sont les suivantes:

a) il est recommandé que le fournisseur CSP dispose de méthodes de contrôle d'accès appropriées pour les serveurs de stockage des données de surveillance;

b) il est recommandé que le fournisseur CSP détermine une période maximale pour la conservation des données de surveillance;

c) il est recommandé que le fournisseur CSP dispose de méthodes de chiffrement appropriées pour les données de surveillance.

Le Tableau 10-2 fournit un résumé mettant en correspondance les menaces de sécurité liées au stockage des données de surveillance et les exigences de sécurité.

Tableau 10-2 – Stockage des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Perte et fuite de données	a), b), c)
Indisponibilité des services	a), c)

10.3 Exigences de sécurité pour l'utilisation des données de surveillance

Les exigences de sécurité pour l'utilisation des données de surveillance sont les suivantes:

a) il est obligatoire que le fournisseur CSP précise clairement au client CSC la façon dont les données de surveillance vont être utilisées;

b) il est recommandé que le fournisseur CSP fournisse au client CSC une déclaration officielle sur l'utilisation des données de surveillance, comme cela est illustré dans la Figure 10-1.

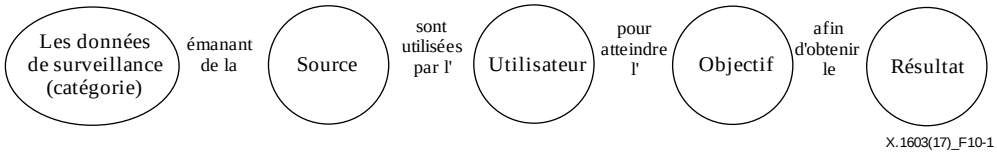

Figure 10-1 – Déclaration recommandée pour l'utilisation des données de surveillance

c) il est obligatoire que le fournisseur CSP envoie une notification au client CSC et obtienne sa permission avant d'utiliser les données de surveillance à d'autres fins que celles prévues;

d) il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit de l'utilisation des données de surveillance.

Le Tableau 10-3 fournit un résumé mettant en correspondance les menaces de sécurité liées à l'utilisation des données de surveillance et les exigences de sécurité.

Tableau 10-3 – Utilisation des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Utilisation abusive des données	a), b), c), d)
Menaces internes	a), b), c), d)
Vulnérabilité du système	d)
Ecoutes illicites	d)

10.4 Exigences de sécurité pour la migration des données de surveillance

Les exigences de sécurité pour la migration des données de surveillance sont les suivantes:

a) il est recommandé que le fournisseur CSP envoie une notification au client CSC concernant la migration des données de surveillance;

b) il est obligatoire que le fournisseur CSP assure la transmission sécurisée des données de surveillance lors de la migration;

c) il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit des opérations de migration des données de surveillance.

Le Tableau 10-4 fournit un résumé mettant en correspondance les menaces de sécurité liées à la migration des données de surveillance et les exigences de sécurité.

Tableau 10-4 – Migration des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Utilisation abusive des données	a), c)
Usurpation d'identité	b), c)
Interception et falsification	b), c)

10.5 Exigences de sécurité pour l'analyse des données de surveillance

Les exigences de sécurité pour l'analyse des données de surveillance sont les suivantes:

a) il est obligatoire que le fournisseur CSP envoie une notification au client CSC concernant l'objectif de l'analyse des données de surveillance;

b) il est obligatoire que le fournisseur CSP mette en place des mesures de protection contre les vulnérabilités du système d'analyse des données de surveillance. Le fournisseur CSP devrait, par exemple, prévenir la perte et la fuite de données dans le système d'analyse des données de surveillance;

Le Tableau 10-5 fournit un résumé mettant en correspondance les menaces de sécurité liées à l'analyse des données de surveillance et les exigences de sécurité.

Tableau 10-5 – Analyse des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Utilisation abusive des données	a)
Vulnérabilité du système	b)
Attaque DoS	b)

10.6 Exigences de sécurité pour la présentation des données de surveillance

Les exigences de sécurité pour la présentation des données de surveillance sont les suivantes:

a) il est obligatoire que le fournisseur CSP préserve l'intégrité et l'exactitude des données de surveillance présentées;

b) il est obligatoire que le fournisseur CSP mette en place des mesures d'authentification pour protéger l'accès à la présentation des données de surveillance;

c) il est obligatoire que le fournisseur CSP mette en place des mesures de protection contre les vulnérabilités du système de présentation des données de surveillance. Le fournisseur CSP peut, par exemple, utiliser des méthodes de test d'intrusion pour prévenir les vulnérabilités du système de présentation des données de surveillance.

Le Tableau 10-6 fournit un résumé mettant en correspondance les menaces de sécurité liées à la présentation des données de surveillance et les exigences de sécurité.

Tableau 10-6 – Présentation des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Utilisation abusive des données	a), b)
Vulnérabilité du système	b), c)
Représentation erronée	a), b), c)

10.7 Exigences de sécurité pour la destruction des données de surveillance

Les exigences de sécurité pour la destruction des données de surveillance sont les suivantes:

a) il est obligatoire que le fournisseur CSP dispose de méthodes de destruction des données de surveillance appropriées;

b) il est obligatoire que le fournisseur CSP prenne des mesures pour prévenir la destruction involontaire des données de surveillance;

c) il est obligatoire que le fournisseur CSP prenne des mesures pour prévenir la destruction incomplète des données de surveillance;

d) il est obligatoire que le fournisseur CSP efface toute clé de chiffrement propre à un client CSC pour les données chiffrées;

e) il est obligatoire que le fournisseur CSP détruise les copies des données de surveillance;

f) il est obligatoire que le fournisseur CSP envoie une notification au client CSC concernant la destruction des données de surveillance.

Le Tableau 10-7 fournit un résumé mettant en correspondance les menaces de sécurité liées à la destruction des données de surveillance et les exigences de sécurité.

Tableau 10-7 – Destruction des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Usurpation d'identité	a), b), c), d), e), f)
Vulnérabilité du système d'exploitation	b), c), d), e), f)

10.8 Exigences de sécurité pour la sauvegarde des données de surveillance

Les exigences de sécurité pour la sauvegarde des données de surveillance sont les suivantes:

a) il est obligatoire que le fournisseur CSP dispose de méthodes de sauvegarde pour prévenir la perte de données de surveillance;

b) il est obligatoire que le fournisseur CSP préserve l'intégrité et l'exactitude des données de surveillance restaurées;

c) il est obligatoire que le fournisseur CSP prévoie la journalisation et l'audit de la restauration des données de surveillance.

Le Tableau 10-8 fournit un résumé mettant en correspondance les menaces de sécurité liées à la sauvegarde des données de surveillance et les exigences de sécurité.

Tableau 10-8 – Sauvegarde des données de surveillance: mise en correspondance des menaces de sécurité et des exigences de sécurité

Menaces de sécurité	Exigences de sécurité
Vulnérabilité du système d'exploitation	a), b), c)

Bibliographie

[b-UIT-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*.

[b-UIT-T X.810] Recommandation UIT-T X.810 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

[b-UIT-T X.1601] Recommandation UIT-T X.1601 (2015), *Cadre de sécurité applicable à l'informatique en nuage*.

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014), *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-UIT-T Y.3502] Recommandation UIT-T Y.3502 (2014), *Technologies de l'information – Informatique en nuage – Architecture de référence*.

[b-ISO/CEI 19440] ISO/CEI 19440 (2007), *Entreprise intégrée – Constructions pour la modélisation d'entreprise*.

[b-ISO/CEI 19944] ISO/CEI 19944 (2016), *Technologies de l'information – Services et dispositifs en nuage: Débits, catégories et utilisation des données*.

[b-ISO/CEI 20000-1] ISO/CEI 20000-1 (2011), *Technologies de l'information – Gestion des services – Partie 1: Exigences du système de management des services*.

[b-ISO/CEI 27000] ISO/CEI 27000 (2012), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/CEI 27729] ISO/CEI 27729 (2012), *Information et documentation – Code international normalisé des noms (ISNI)*.

[b-ISO/CEI 29100] ISO/CEI 29100 (2011), *Technologies de l'information – Techniques de sécurité – Cadre privé.*

[b-NIST-SP-800-30] Publication spéciale du NIST 800-30 (2012), *Guide for Conducting Risk Assessments.*

[b-NIST-SP-800-53] Publication spéciale du NIST 800-53 Rév.3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations.*

[b-NIST-SP-800-125] Publication spéciale du NIST 800-125 (2011), *Guide to Security for Full Virtualization Technologies.*

[b-NIST-SP-800-145] Publication spéciale du NIST 800-145 (2011), *The NIST Definition of Cloud Computing*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2018