Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1750

(09/2020)

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

Sécurité des données – Sécurité des mégadonnées

Lignes directrices relatives à la sécurité des mégadonnées en tant que service pour les fournisseurs de services de mégadonnées

Recommandation UIT-T X.1750

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange 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 œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	**X.1750–X.1759**
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1750

Lignes directrices relatives à la sécurité des mégadonnées en tant que service pour les fournisseurs de services de mégadonnées

Résumé

Les mégadonnées en tant que service (BDaaS) sont une catégorie de service en nuage qui permet aux clients des services en nuage de collecter, stocker, analyser, visualiser et gérer les mégadonnées, comme indiqué dans la Recommandation UIT-T Y.3600. Compte tenu de l'augmentation spectaculaire des volumes de données et de l'évolution rapide des activités liées aux mégadonnées, l'infrastructure des mégadonnées s'est imposée comme l'installation centrale pour la fourniture de services BDaaS. En conséquence, des questions importantes concernant la sécurité des services BDaaS se font jour. À titre d'exemple, lors de la conception de logiciels de mégadonnées à code source ouvert, la sécurité n'est pas toujours prise en considération dès le début. De plus, il se peut que les nouvelles technologies mises au point pour l'analyse des mégadonnées se traduisent par un non-respect des mesures classiques de protection de la sécurité. La Recommandation UIT-T X.1750 contient une analyse des problèmes de sécurité que rencontrent les services BDaaS et définit les rôles et les responsabilités liés à la sécurité dans la fourniture des services BDaaS, ainsi qu'un cadre de sécurité applicable à une infrastructure de mégadonnées. Cette Recommandation précise en outre les mesures de protection de la sécurité à respecter pour les services et les composantes associés aux services BDaaS.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1750	03-09-2020	17	11.1002/1000/14266

Mots clés

Mégadonnées en tant que service, lignes directrices relatives à la sécurité, mesures de sécurité.

* 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 on 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Recommandation UIT-T X.1750

Lignes directrices relatives à la sécurité des mégadonnées en tant que service pour les fournisseurs de services de mégadonnées

1 Champ d'application

La présente Recommandation contient une analyse des problèmes de sécurité que rencontrent les mégadonnées en tant que service (BDaaS) et énonce des lignes directrices applicables aux fournisseurs de services de mégadonnées (BDSP) pour sécuriser les services BDaaS. Elle définit les rôles et les responsabilités liés à la sécurité des composantes des services BDaaS, et un cadre de sécurité applicable aux infrastructures de mégadonnées, qui incluent les plates-formes, les applications, les analyses, les interfaces et l'écosystème des services BDaaS. De plus, la présente Recommandation précise les mesures de protection de la sécurité qui devraient être prises en ce qui concerne les activités ou les composantes associées aux services BDaaS.

La présente Recommandation constitue une description de haut niveau des exigences de sécurité applicables à la mise en œuvre des services BDaaS axée sur les services BDaaS. Les services BDaaS font intervenir des fournisseurs d'infrastructures de mégadonnées (BDIP) et des fournisseurs d'applications de mégadonnées (BDAP). Les lignes directrices à l'intention de ces deux types de fournisseurs ainsi que les orientations détaillées sur la mise en œuvre des services BDaaS n'entrent pas dans le cadre de la présente Recommandation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

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

[UIT-T X.1631] Recommandation UIT-T X.1631 (2015), *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage*.

[UIT-T X.1641] Recommandation UIT-T X.1641 (2016), *Lignes directrices pour la sécurité des données des clients de services en nuage*.

[UIT-T Y.3600] Recommandation UIT-T Y.3600 (2015), *Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage*.

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

[ISO/CEI 27036-3] ISO/CEI 27036-3:2013, *Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur – Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information.*

[ISO 28000] ISO 28000:2007, *Spécifications relatives aux systèmes de management de la sûreté de la chaîne d'approvisionnement*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 mégadonnées [UIT-T Y.3600]: modèle qui permet de collecter, stocker, gérer, analyser et visualiser d'immenses ensembles de données ayant des caractéristiques hétérogènes, éventuellement en respectant des contraintes de temps réel.

NOTE – Parmi les exemples de caractéristiques des ensembles de données, on peut citer un grand volume, une grande rapidité, une grande diversité, etc.

3.1.2 mégadonnées en tant que service (BDaaS) [UIT-T Y.3600]: catégorie de service en nuage, dans laquelle les capacités fournies au client du service en nuage sont celles de collecter, stocker, analyser, visualiser et gérer les données au moyen de technologies de mégadonnées.

3.1.3 provenance des mégadonnées [b-UIT-T Y.3602]: information qui retrace le cheminement historique des données en fonction des opérations du cycle de vie des données dans un écosystème des mégadonnées.

3.1.4 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, approvisionnées et administrées à la demande et en libre-service.

3.1.5 service en nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes via l'informatique en nuage invoquées à l'aide d'une interface définie.

3.1.6 métadonnées [b-UIT-T M.3030]: données qui décrivent d'autres données.

3.1.7 problème de sécurité [UIT-T X.1601]: "souci" de sécurité autre qu'une menace directe de sécurité découlant de la nature et de l'environnement d'exploitation des services de nuage, y compris les menaces "indirectes".

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

3.1.9 vulnérabilité [b-NIST-SP-800-30]: faiblesse 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 le terme suivant:

3.2.1 actif de données: ressource de données enregistrée au format électronique, possédée ou contrôlée par une organisation.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ABAC contrôle d'accès fondé sur des attributs (*attribute-based access control*)

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

BDaaS mégadonnées en tant que service (*big data as a service*)

BDAP fournisseur d'applications de mégadonnées (*big data application provider*)

BDIP fournisseur d'infrastructure de mégadonnées (*big data infrastructure provider*)

BDSN partenaire de services de mégadonnées (*big data service partner*)

BDSP fournisseur de services de mégadonnées (*big data service provider*)

BDSU utilisateur de services de mégadonnées (*big data service user*)

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

DP fournisseur de données (*data provider*)

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

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

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

SDK kit de développement logiciel (*software development kit*)

SSL couche de connexion sécurisée (*secure socket layer*)

TI technologies de l'information, informatique

TLS sécurité dans la couche transport (*transport layer security*)

USB bus série universel (*universal serial bus*)

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. Ces mots n'impliquent pas que la mise en œuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau ou le fournisseur de service. Ils signifient plutôt que le fabricant peut incorporer la caractéristique à titre facultatif et revendiquer néanmoins la conformité avec la spécification.

6 Menaces et problèmes de sécurité concernant les mégadonnées en tant que service

Le présent paragraphe contient une description des menaces et des problèmes de sécurité concernant les services BDaaS. Les services BDaaS basés sur l'informatique en nuage sont définis dans la Recommandation [UIT-T Y.3600]. Les problèmes de sécurité concernant les environnements de l'informatique en nuage décrits dans le paragraphe 8 de la Recommandation [UIT-T X.1601] devraient être pris en considération dans le cas des services BDaaS. La présente Recommandation contient alors une description des menaces et des problèmes de sécurité concernant des capacités et des services spécifiques des services BDaaS, c'est-à-dire les plates-formes de mégadonnées en tant que service et les logiciels liés aux mégadonnées en tant que service (en reconnaissant que l'écosystème des services BDaaS englobe les fournisseurs de données (DP) ainsi que les fournisseurs BDAP et BDIP, notamment:

– les vulnérabilités des infrastructures de mégadonnées et le non-respect des mesures de sécurité;

– les problèmes de stockage et d'audit résultant de données non structurées;

– la sécurité et la régulation de l'interface entre les applications, les plates-formes et le flux de service;

– d'autres préoccupations liées à la sécurité, comme la confiance, l'authentification et la visualisation.

La Figure 6-1 présente une architecture des problèmes de sécurité concernant les services BDaaS.

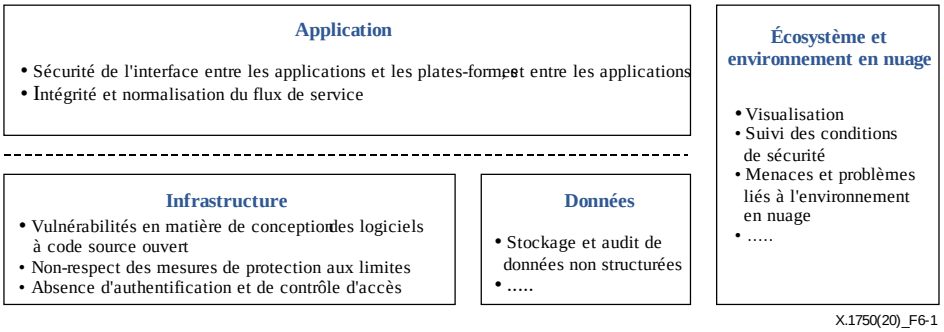

Figure 6-1 – Problèmes de sécurité des mégadonnées en tant que service

6.1 Problèmes de sécurité pour une infrastructure de mégadonnées

Une infrastructure de mégadonnées peut se présenter sous la forme de plusieurs composantes obtenues dans le commerce ou à code source ouvert. Il est possible que la sécurité ne soit pas prise en considération dès le début de la conception de certaines de ces composantes, ce qui peut engendrer des risques de sécurité, notamment les suivants:

– l'insécurité du code source et l'absence de mécanisme de sécurité dans les composantes à code source ouvert;

– des caractéristiques de plate-forme ouverte et interdomaines qui brouillent les limites traditionnelles de la sécurité, conduisant à l'absence de mesures de protection aux limites; et

– l'absence de mécanismes d'authentification et de contrôle d'accès appropriés pour les différents rôles peut conduire à des utilisations abusives.

6.2 Problèmes de sécurité pour les applications des mégadonnées

Une infrastructure de mégadonnées intègre un certain nombre d'applications très centralisées avec des modèles de services compliqués. Les problèmes de sécurité concernant les applications des mégadonnées sont notamment les suivants:

– l'absence possible de vérifications de sécurité et d'une commande de transmission pour les interfaces de programmation d'application (API), les kits de développement logiciel (SDK) et les interfaces entre les applications; et

– la nécessité de suivre, vérifier et localiser l'exécution des applications d'utilisateur pour garantir la sécurité logique opérationnelle.

6.3 Problèmes de sécurité pour les données

L'infrastructure et les applications des mégadonnées gèrent de très grandes quantités de données. Dans un écosystème des mégadonnées, il existe plusieurs types de données: les données structurées, semi-structurées et non structurées. Les données structurées sont souvent stockées dans des bases de données qui peuvent être organisées en fonction de modèles différents, par exemple le modèle relationnel, le modèle de document, le modèle clé-valeur et le modèle graphique. Les données semi-structurées ne sont pas conformes à la structure formelle des modèles de données, mais contiennent des balises ou des marqueurs pour identifier les données. Enfin, les données non structurées n'ont pas de modèle de données prédéfini et ne sont organisées d'aucune manière définie. Différents formats, par exemple le format texte, tableur, vidéo, audio, image et plan, peuvent exister parmi tous les types

de données (voir la Recommandation [UIT-T Y.3600]). Ces données sont utilisées dans le cadre du stockage, de l'analyse, du calcul et d'autres phases des services de données. Les problèmes de sécurité concernant les données sont notamment les suivants:

– l'exigence de mesures de sécurité (y compris des contrôles d'accès) pour garantir la confidentialité des données, tout en continuant à favoriser l'exploitation efficace des données;
– l'audit des données non structurées;
– le risque de fuite des informations personnelles si les données sont ouvertes ou partagées;
– la nécessité d'appliquer les mesures de sécurité traditionnelles décrites dans la Recommandation [UIT-T X.1601] pour les métadonnées, dans la mesure où elles ont les mêmes caractéristiques que les données publiées sur le web.

Les problèmes de sécurité concernant la gestion de la provenance des mégadonnées sont notamment les suivants: informations contaminées ou manipulées de manière malveillante à travers la chaîne de traitement de la provenance, entités non habilitées dans le traitement ou l'échange de données sur la provenance, codes de traitement inauthentiques pour la provenance des données, et problèmes de sécurité concernant les données sur la provenance.

6.4 Problèmes de sécurité pour l'écosystème des mégadonnées en tant que service

D'après la Recommandation [UIT-T Y.3600], un écosystème des services BDaaS est composé de parties ou composantes jouant des rôles et des sous-rôles différents qui fournissent et consomment des services de mégadonnées. L'écosystème des services BDaaS est nécessaire pour prévoir, élaborer et appliquer des mesures de sécurité dans la construction, l'exploitation, l'audit et d'autres phases de la provenance des services. Les problèmes de sécurité concernant les services de mégadonnées sont notamment les suivants:

– nécessité de surveiller en permanence les actions des utilisateurs, les conditions du réseau, l'état des ressources, etc. pour faire face aux menaces changeantes;
– vecteurs émergents de nouvelles menaces et absence de mécanismes potentiels de protection;
– incapacité d'établir une relation de confiance entre différents acteurs, y compris les propriétaires de données et les dispositifs (pour recueillir des données);
– sécurité de l'instanciation de la virtualisation, par exemple la configuration de la sécurité et l'intégrité de l'image virtuelle;
– existence possible d'une chaîne logistique compliquée dans un écosystème des mégadonnées. Même un contractant qui n'est pas directement lié par contrat avec une organisation peut avoir une influence sur la continuité de ses activités. Les risques liés à la chaîne logistique devraient être analysés et des mesures nécessaires devraient être prises, notamment les mesures de sécurité énoncées dans les Normes [ISO/CEI 27000] et [ISO 28000].

7 Concepts de haut niveau des considérations relatives à la sécurité des mégadonnées en tant que service et rôle des fournisseurs BDSP

La Recommandation [UIT-T Y.3600] définit une architecture des technologies des mégadonnées générale, qui porte sur plusieurs niveaux et qui est constituée de composantes de fonction logique. Sur la base de cette architecture, les capacités de sécurité des services des mégadonnées couvrent à la fois la sécurité des systèmes et la sécurité des données.

Du point de vue des systèmes, les exigences de sécurité des services BDaaS portent sur les capacités de chaque module de fonction qui se rapporte 1) à l'infrastructure des mégadonnées; 2) à la gestion des applications des mégadonnées; 3) à la sécurité de l'interface; et 4) à la gestion et au maintien de la sécurité de la plate-forme des mégadonnées (écosystème des services BDaaS).

En particulier, selon la description de la Recommandation [UIT-T Y.3600], les services BDaaS comportent deux composantes essentielles:

– Les fournisseurs BDIP peuvent utiliser les services en nuage des types de capacité de l'infrastructure en nuage, comme le calcul en tant que service, le stockage de données en tant que service, l'infrastructure en tant que service et le réseau en tant que service, afin de fournir des services de mégadonnées tels que la collecte, le traitement et la gestion des données.
– Les fournisseurs BDAP effectuent des analyses de données et des visualisations, et exécute d'autres applications des mégadonnées.

Du point de vue des données, les exigences de sécurité portent sur chaque activité dans le processus de développement des activités liées aux services des mégadonnées. De plus, les capacités des services des mégadonnées incluent également des exigences applicables à la sécurité des métadonnées et de la chaîne d'approvisionnement des données.

Du point de vue du système des services BDaaS, la Recommandation [UIT-T Y.3600] identifie le contexte du système, notamment les rôles et les activités ainsi que les flux de données et de service.

En ce qui concerne les rôles décrits dans la Recommandation [UIT-T Y.3600], les services BDaaS sont fournis par les fournisseurs BDSP, qui sont chargés de garantir la sécurité des services BDaaS et de réduire les risques. Il est recommandé aux fournisseurs BDSP (BDIP et BDAP) de prendre en compte à la fois la sécurité du système et la sécurité des données pour mener des activités liées aux services BDaaS.

8 Mesures de sécurité applicables aux mégadonnées en tant que service

8.1 Mesures de sécurité applicables à une infrastructure des mégadonnées

8.1.1 Sécurité des actifs d'un système

8.1.1.1 Exigences générales

Les fournisseurs BDSP devront:

– élaborer des stratégies de gestion de la sécurité des actifs d'un système, et préciser les objectifs et les principes de la sécurité des actifs d'un système;
– élaborer des politiques et des procédures de construction et de gestion de l'exploitation des actifs d'un système, portant notamment sur la planification, la conception, l'achat, le développement, l'exploitation, la conservation et la destruction;
– établir un mécanisme d'enregistrement des actifs d'un système, dresser une liste des actifs d'un système, définir la question de la responsabilité de la sécurité des actifs d'un système et les parties concernées, et mettre à jour régulièrement les informations sur les actifs d'un système;
– établir et mettre en œuvre des procédures de classification et d'étiquetage des actifs d'un système;
– effectuer régulièrement des audits et des mises à jour des actifs des technologies de l'information et des politiques de gestion de la sécurité.

8.1.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– identifier les contrôles de gestion d'actifs disponibles, tels que ceux définis dans la Recommandation [UIT-T X.1631], pour effectuer un inventaire et un enregistrement des composantes, effectuer un audit et contrôler les actifs du système;
– élaborer des procédures d'évaluation des risques des actifs pour le système des mégadonnées, par exemple mettre en œuvre un processus permettant d'identifier les composantes des produits ou services qui sont essentielles pour préserver la fonctionnalité, et qui requièrent donc une attention et une surveillance renforcées;

– élaborer des procédures d'évaluation de la sécurité pour la chaîne d'approvisionnement, telles que celles définies dans la Norme [ISO/CEI 27036-3]. Il s'agit notamment d'évaluer les risques liés au fait que des composantes ne sont plus disponibles et les processus systématiques et reproductibles d'intervention en cas de vulnérabilité.

8.1.2 Sécurité des actifs de données

8.1.2.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer des stratégies de gestion de la sécurité des actifs de données, et préciser les objectifs et les principes de la gestion de la sécurité des actifs de données;

– établir des mécanismes et des procédures de gestion de la sécurité s'appliquant au cycle de vie des actifs de données;

– établir des méthodes de classification et de gradation et des directives opérationnelles relatives aux actifs de données en fonction de la valeur et de l'importance des actifs de données;

– établir des mécanismes d'approbation des changements concernant les stratégies, les procédures, les méthodes et les directives opérationnelles relatives à la classification et à la gradation des données;

– établir des spécifications de sécurité, des mécanismes et des procédures de gestion concernant la confidentialité, l'intégrité et la disponibilité des actifs de données (exemples: stratégie de mot de passe, gestion de clé);

– dresser une liste des actifs de données, et identifier la question de la responsabilité de la sécurité des données et les parties concernées;

– effectuer régulièrement des audits et des mises à jour des stratégies de gestion de la sécurité des actifs de données et des procédures pertinentes.

8.1.2.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– élaborer des principes de gouvernance de la sécurité et des politiques d'intégration des données pour tous les types de ressources de données internes et externes;

– établir un étiquetage correspondant, un contrôle d'accès à plusieurs niveaux, un chiffrement et un déchiffrement des données, une désensibilisation des données et d'autres stratégies de sécurité en conformité avec la sensibilité des actifs des données.

8.1.3 Sécurité du processus de la chaîne d'approvisionnement des données

8.1.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– préciser les objectifs, les principes et le champ d'application de la gestion de la sécurité de la chaîne d'approvisionnement des données;

– élaborer des politiques et des procédures de gestion de la sécurité de la chaîne d'approvisionnement des données, y compris des critères de gestion de la sécurité assurée par les participants à la chaîne d'approvisionnement des données;

– donner des précisions sur les buts, les modèles d'approvisionnement et les responsabilités des participants en matière de sécurité des données dans la chaîne d'approvisionnement des données au moyen d'accords de coopération;

– enregistrer les équipements et les applications d'acquisition et de diffusion des données, consigner les comportements d'acquisition et de diffusion et effectuer un audit de ceux-ci;

– effectuer un audit du comportement de consommation des données des participants à la chaîne d'approvisionnement des données;
– établir un mécanisme de normalisation des sources de données et des spécifications relatives à l'interface dans la chaîne d'approvisionnement des données, journaliser les opérations importantes et effectuer un audit de celles-ci;
– établir une structure organisationnelle de l'exploitation et de la gestion de la chaîne d'approvisionnement, un modèle de données principal de la chaîne d'approvisionnement, un mécanisme de traitement de la qualité des données et un mécanisme de traçabilité des données;
– préciser les responsabilités en matière de sécurité de la chaîne d'approvisionnement des données et garantir l'authenticité et la disponibilité des services de données connexes;
– veiller à ce que des mesures de sécurité soient déployées dans les processus d'approvisionnement des données, comme l'échange de données et l'utilisation des données;
– établir des catalogues de la chaîne d'approvisionnement des données et des dictionnaires sur les sources des données, et identifier la partie responsable de la sécurité du processus d'approvisionnement des données;
– veiller à la fiabilité des renseignements dans toute la chaîne de traitement de la provenance;
– définir les entités responsables du traitement de la provenance des données;
– mettre en œuvre des mécanismes d'authentification pour garantir l'authenticité des entités dans la chaîne de traitement et d'échange des données sur la provenance;
– veiller à l'authenticité des codes pour la provenance des données et conserver cette authenticité au moyen de la mise à jour des codes;
– veiller à la confidentialité, à l'intégrité et à la disponibilité des données sur la provenance; ces exigences de sécurité sont décrites dans la Recommandation [UIT-T X.1601].

8.1.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– préciser les exigences relatives aux capacités des services de données applicables aux différents participants à la chaîne d'approvisionnement des données en fonction de leur rôle respectif dans l'écosystème de la chaîne opérationnelle des données;
– examiner régulièrement les capacités de gestion de la sécurité des données des participants à la chaîne d'approvisionnement des données, et évaluer les risques auxquels ils sont exposés en matière de sécurité;
– évaluer régulièrement les risques en matière de sécurité de l'ensemble du cycle de vie de la chaîne d'approvisionnement des données.

8.1.4 Sécurité des métadonnées

Les exigences de sécurité des données des clients de services en nuage (CSC) pertinentes, définies dans la Recommandation [UIT-T X.1641], devraient être prises en considération.

8.1.4.1 Exigences générales

Les fournisseurs BDSP doivent:

– établir des dictionnaires de données et des pratiques de gestion pertinentes en fonction de l'architecture de l'entreprise et des services de données, dont le domaine des données, le type de champ, la structures des tableaux, ainsi que le mode de stockage logique et physique;
– établir des métadonnées relatives à la sécurité et des pratiques de gestion pertinentes en fonction de l'architecture de la sécurité des mégadonnées, dont la politique de mot de passe, la liste des autorités et les spécifications d'autorisation;

– établir une stratégie de contrôle d'accès aux métadonnées, définir les rôles des métadonnées et les mécanismes de contrôle d'autorisation;
– établir des procédures d'audit de l'exploitation des métadonnées.

8.1.4.2 Exigences renforcées

Les fournisseurs BDSP devraient:
– bâtir des systèmes de gestion des métadonnées pour assurer la gestion de l'unification des métadonnées des services de mégadonnées;
– établir un mécanisme d'évaluation automatique applicable aux attributs de la sécurité des métadonnées en fonction de la stratégie de classification et d'évaluation des actifs;
– établir une stratégie d'étiquetage, y compris la liaison des données et du propriétaire des données, en fonction des exigences de sécurité des métadonnées.

8.2 Mesures de sécurité pour les applications des mégadonnées

8.2.1 Acquisition des ressources de plates-formes

8.2.1.1 Exigences générales

Les fournisseurs BDSP doivent:
– veiller à ce que les utilisateurs des services des mégadonnées (BDSU) soient conscients et informés du fait que les actifs d'un système sont accessibles via une application, comme une connexion au réseau, un service de localisation et une liste de ressources matérielles comme un bus série universel (USB) et le Bluetooth;
– veiller à ce que les utilisateurs BDSU soient conscients et informés du fait que les actifs de données sensibles d'un système sont accessibles via une application, comme des carnets d'adresses, des journaux système et d'autres sources d'informations sensibles;
– veiller à ce qu'un motif suffisant soit invoqué pour demander à accéder aux ressources via une application, comme indiqué dans les documents fournis par le développeur de l'application.

8.2.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:
– veiller à ce qu'une application limite les communications de réseau internes et externes non nécessaires ou les communications de réseau à l'initiative de l'utilisateur selon les exigences opérationnelles.

8.2.2 Autorisation et contrôle d'accès

8.2.2.1 Exigences générales

Les fournisseurs BDSP doivent:
– établir une granularité des autorisations d'accès physique et logique, et un mécanisme de spécification et de contrôle des applications des mégadonnées, pour veiller à ce que les accès aux données liées aux services des mégadonnées et aux actifs des systèmes soient dûment autorisés;
– établir des mesures relatives à l'autorisation et au contrôle d'accès basées sur les stratégies de gestion des actifs et les étiquettes des actifs, et des attributs de sécurité, pour veiller à ce qu'une application des mégadonnées dispose des capacités de gestion du contrôle d'accès à granularité fine;
– élaborer une stratégie de contrôle des flux d'informations pour contrôler les opérations d'importation, d'exportation et de partage des données de l'infrastructure des mégadonnées

entre les différentes applications des mégadonnées ou entre une application des mégadonnées et un système informatique externe;

– mettre en œuvre une autorisation dûment approuvée de l'accès des personnes, des groupes, des rôles, des dispositifs et des applications liés aux services des mégadonnées aux données et aux actifs d'un système;

– offrir la possibilité qu'une stratégie en matière d'autorisation d'accès soit autodéfinie par l'utilisateur sur la base des exigences relatives aux services, et que l'autorisation d'effectuer des audits soit donnée par chaque utilisateur sur la base des exigences relatives aux services, pour veiller à ce que son accès soit limité à la portée minimale conformément aux exigences des scénarios de service.

8.2.2.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– surveiller et contrôler les sessions d'accès à distance automatiquement pour détecter les attaques de réseau et veiller à l'exécution de la politique d'accès à distance;

– fournir un moteur de contrôle d'accès basé sur les attributs (ABAC) et des fonctionnalités de gestion d'autorisation et de contrôle d'accès orientées sur les objets des données, ainsi que des fonctionnalités comme le point d'administration de politique, le point de décision de politique, le point d'application de politique et le point d'accès de politique.

8.2.3 Surveillance du comportement des applications

8.2.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– établir des stratégies et des procédures de surveillance du comportement des applications des mégadonnées qui s'appliquent à l'ensemble du cycle de vie des données;

– aider les utilisateurs à personnaliser les règles de surveillance qui peuvent appuyer la surveillance et le signalement des opérations anormales concernant des données critiques;

– avoir la possibilité d'enregistrer, de pointer et d'analyser les informations relatives à un comportement anormal d'une application.

8.2.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– établir des mécanismes de gestion de la surveillance du comportement des applications centrés sur les régulateurs et les utilisateurs avec des exigences spécifiques, et fournir une interface de surveillance en ligne après autorisation;

– créer une plate-forme pour enregistrer et analyser le comportement des applications des mégadonnées, et offrir des capacités d'analyse de sécurité en fournissant des composantes d'identification du comportement de l'utilisateur et d'extraction, ou des interfaces pour les protocoles de communication des services des mégadonnées;

– fournir des systèmes de spécification de la surveillance du comportement et des lignes directrices opérationnelles.

8.2.4 Stratégies et procédures relatives à la sécurité des applications

Les fournisseurs BDSP doivent:

– établir une politique de gestion des versions pour les applications des services des mégadonnées sous la forme d'une procédure d'autorisation par écrit définissant les responsabilités relevant des rôles pertinents – le document d'autorisation devrait indiquer le

nom, la version, la source, le développeur, la fonction, l'emplacement du déploiement, le résultat de l'évaluation de la sécurité et les exigences de sécurité spécifiques des applications;

– donner des précisions sur la protection de la transmission des données entre les applications et l'infrastructure des mégadonnées, ainsi que d'autres produits informatiques authentiques; par exemple, appliquer des systèmes de sécurité comme la couche de connexion sécurisée (SSL) ou la sécurité dans la couche transport (TLS) pour chiffrer les données sensibles dans la transmission;

– vérifier les signatures électroniques des paquetages d'installation des applications et des paquetages de mise à jour;

– veiller à ce qu'une application puisse interroger la version actuelle du logiciel exécuté, de manière autonome ou en utilisant les fonctions pertinentes de l'infrastructure des mégadonnées;

– veiller à ce qu'une application puisse prendre en charge des opérations d'erreurs prévisibles sans que cela ait une incidence sur les travaux normaux des écosystèmes des mégadonnées;

– établir une politique de mise à jour des applications des mégadonnées et de gestion des correctifs, et s'assurer que les applications rechercheront les mises à jour et installeront des correctifs de composant;

– suivre les spécifications de conception de la sécurité des applications des mégadonnées, en évitant les entrées qui violent ou contournent les règles de sécurité et les entrées non spécifiées;

– concevoir des mécanismes visant à prévenir l'exploitation de vulnérabilités des applications des mégadonnées; par exemple, éviter d'attribuer de l'espace mémoire qui a à la fois les permissions d'écriture et d'exécution, attribuer de l'espace mémoire avec les permissions d'écriture et d'exécution seulement pour des fonctions de compilation à la volée.

8.2.5 Stockage des justificatifs

8.2.5.1 Exigences générales

Les fournisseurs BDSP doivent:

– définir une méthode de stockage persistant des justificatifs d'identité des applications, notamment utiliser une fonction de plate-forme plutôt que de stockage pour stocker tous les justificatifs d'identité en sécurité, ou exécution de la fonction de stockage sécurisé des justificatifs d'identité par l'application elle-même;

– préciser les informations relatives aux justificatifs d'une application, par exemple la clé, l'infrastructure de clé publique (PKI), la clé privée ou le mot de passe;

– préciser les méthodes de protection de la sécurité et les mesures de contrôle pour recueillir, stocker et utiliser les informations d'identification personnelle;

– établir un processus d'évaluation applicable à la méthode de stockage des justificatifs d'une application, pour veiller à ce qu'elle soit conforme aux stratégies de sécurité et aux exigences procédurales applicables aux systèmes pour les services des mégadonnées.

8.2.5.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– s'assurer que l'objectif du stockage persistant des justificatifs d'identité et les méthodes y afférentes sont mentionnés dans les documents de spécification de la sécurité.

8.2.6 Identité et authentification

8.2.6.1 Exigences générales

Les fournisseurs BDSP doivent:

– offrir la possibilité de gérer l'identité de l'utilisateur automatiquement pour déterminer les informations sur l'identité de l'utilisateur dans les applications des mégadonnées, afin d'assurer des relations de mappage entre l'identification de l'utilisateur et les informations relatives à l'autorisation dans la couche application;

– authentifier l'identité de l'utilisateur en utilisant plus d'une technique d'authentification pour l'exploitation de données importantes ou de modules importants;

– présenter les informations potentiellement utiles sur l'utilisation des services des systèmes de mégadonnées accessibles au public, comme l'affichage de la date et de l'heure de la dernière connexion, ou de l'emplacement depuis lequel la connexion la plus récente a eu lieu.

8.2.6.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– authentifier l'identité de l'utilisateur en utilisant plus d'une technique d'authentification dans toutes les applications pour un utilisateur occupant une position clé, avec au moins une technique basée sur une méthode de certification biométrique ou numérique;

– utiliser la méthode de fédération du langage de balisage d'assertion de sécurité (SAML) pour spécifier l'identité et le rôle, et ajouter des exigences de sécurité et de respect de la vie privée, ce qui permet de prendre en charge des identités multiples pour accéder aux services des mégadonnées.

8.2.7 Sécurité de la configuration par défaut

Les fournisseurs BDSP doivent:

– veiller, lors de l'utilisation de justificatifs d'identité par défaut ou lorsqu'aucun justificatif d'identité n'est configuré, à ce qu'une application puisse seulement offrir des fonctionnalités essentielles pour configurer une nouvelle identité; par exemple, en utilisant un mot de passe par défaut pour se connecter, un utilisateur est seulement autorisé à accéder à l'interface de modification du mot de passe, et l'application ne devrait proposer aucune autre fonctionnalité tant que le mot de passe par défaut n'a pas été modifié;

– en ce qui concerne les applications, fournir un module fonctionnel plus sécurisé et permettre de renforcer le niveau de sécurité des configurations de sécurité dans le mode d'installation par défaut; par exemple, si une application peut fournir un module de connexion par mot de passe et un module de certification numérique au même moment, dans le cas d'un mode d'installation par défaut, l'application choisit d'installer le module de certification numérique;

– limiter les permissions d'accès par défaut pour les utilisateurs par défaut de l'application; par exemple empêcher un utilisateur avec une permission minimale non-racine de démarrer un programme par défaut;

– veiller à ce qu'une application active la fonctionnalité de configuration de la sécurité du compte utilisateur par défaut, qui inclut la longueur et la complexité du mot de passe, la limite de la durée de service et la stratégie de blocage du compte;

– assurer la mise en place des fonctions nécessaires d'audit des journaux, par exemple la mise à jour de l'installation des composantes ou la modification des paramètres, lorsqu'une application est installée dans la configuration par défaut.

8.2.8 Importation et exportation de données

8.2.8.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer des stratégies et des procédures d'importation et d'exportation des données en tenant compte de facteurs tels que la capacité de stockage, la vitesse de croissance du volume de données, les exigences opérationnelles, le support et l'efficacité de stockage, pour empêcher des pertes de données importantes et réduire les dommages liés à la perte de données;

– mettre en place des stratégies et des mécanismes de gestion de l'exportation des données, des mécanismes d'évaluation de la sécurité de l'importation et de l'exportation des données et un processus d'approbation de l'autorisation;

– établir des spécifications d'identification pour un support de stockage de données exportées – l'identification devra être conforme aux règles de dénomination unifiées, indiquer le nombre de supports, la durée de l'exportation, la période de validité et d'autres informations importantes;

– présenter plusieurs méthodes d'importation et d'exportation des données de granularité multiple, comme la granularité de bases de données, de modèles et d'objets définis par l'utilisateur;

– mener un examen des résultats concernant les données importées et exportées, et veiller à l'intégrité et à la validité des données;

– enregistrer les informations opérationnelles relatives à l'importation et à l'exportation des données, comme les informations sur les opérations, le cycle d'opérations, le nombre de supports, le volume des supports, les situations de transfert et de stockage et la tenue à jour de l'enregistrement des changements importants;

– appliquer des mécanismes de cryptage, un contrôle d'accès et d'autres mesures techniques pour garantir la confidentialité, l'intégrité et la disponibilité des données exportées;

– vérifier régulièrement l'intégrité et la disponibilité des données exportées.

8.2.8.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– mesurer la base de calcul des paramètres indiciels de la gestion de la sauvegarde automatique des données, y compris la durée moyenne de fonctionnement avant défaillance, la durée moyenne de rétablissement et la durée moyenne entre défaillances, et configurer les logiciels correspondants d'importation et d'exportation automatiques des données;

– disposer de la capacité d'importer et d'exporter en ligne des données à distance, et procéder de manière régulière et semi-automatique au stockage de données d'utilisateur à distance;

– sauvegarder automatiquement la recombinaison et la compression des données, notamment selon la popularité des données, et veiller à la disponibilité des données massives;

– disposer d'une fonction de stockage automatique de la compression des données d'utilisateur sauvegardées, selon la fréquence de sauvegarde et de restauration des données.

8.3 Mesures de sécurité pour les interfaces

8.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– fournir des interfaces d'administrateur du système, d'administrateur de la sécurité, d'auditeur de la sécurité et d'autres interfaces de rôle d'utilisateur et des interfaces de rôle de réglementation;

– préciser les exigences de sécurité et les mesures de contrôle de la sécurité pour chaque interface de rôle, par exemple l'authentification de l'identité, l'accès sous autorisation, la signature, l'horodatage et le protocole de sécurité;
– préciser les restrictions de sécurité applicables à l'utilisation de chaque classe d'interface, comme les connexions à distance dont les fonctions et les permissions sont limitées;
– préciser les spécifications de sécurité de l'interface de service, y compris le nom de l'interface, les paramètres de l'interface et les exigences de sécurité applicables à l'interface – les spécifications contiennent des restrictions applicables aux paramètres d'entrée non sécurisés et permettent de traiter des exceptions;
– fournir la capacité d'effectuer des audits des comportements d'accès aux interfaces et des interfaces de service de données configurables;
– adopter des mécanismes de sécurité, tels qu'un canal sécurisé ou un mode de transfert chiffré, pour sécuriser les interfaces de sécurité interdomaines.

8.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– appuyer les exigences d'audit dans le processus d'accès aux interfaces, et fournir des fonctions nécessaires d'audit et de réglementation pour l'accès aux interfaces;
– adopter une méthode de chiffrement des transmissions pour les transmissions aux interfaces à travers des domaines de sécurité dans le système;
– effectuer un suivi et un traitement automatiques essentiels de l'accès aux interfaces.

8.4 Mesures de sécurité pour l'écosystème des mégadonnées en tant que service

8.4.1 Planification de la sécurité

L'étape de planification de la sécurité est divisée en trois sous-étapes:

– analyse des exigences: identification, clarification et définition des exigences opérationnelles et de sécurité;
– élaboration de solutions: quelle(s) solution(s) de sécurité est/sont élaborée(s);
– évaluation de solutions: quelle(s) solution(s) de sécurité est/sont évaluée(s).

Après la dernière sous-étape, le fournisseur BDSP peut soit passer à l'étape de construction de la sécurité pour mise en œuvre, soit revenir à la sous-étape d'élaboration de solution(s) pour ajustement ou amélioration.

8.4.1.1 Analyse des exigences

8.4.1.1.1 Exigences générales

Les fournisseurs BDSP doivent:

– déterminer le champ d'application des activités opérationnelles des services des mégadonnées et des exigences de base correspondantes en matière de sécurité applicables à une infrastructure des mégadonnées;
– identifier les menaces de sécurité, les vulnérabilités et les risques de sécurité spécifiques auxquels fait face une infrastructure des mégadonnées, puis préciser les mesures techniques et de gestion applicables aux services des mégadonnées;
– identifier les priorités en matière de mise en œuvre des exigences de sécurité applicables à l'infrastructure des mégadonnées.

8.4.1.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– élaborer une analyse des exigences de sécurité, examiner la procédure de gestion et veiller à l'intégrité et au caractère raisonnable des exigences de sécurité applicables à une infrastructure des mégadonnées.

8.4.1.2 Élaboration de solutions

8.4.1.2.1 Exigences générales

Les fournisseurs BDSP doivent:

– créer des spécifications techniques de sécurité de l'infrastructure des mégadonnées et décrire clairement la fonction, l'interface et les paramètres de sécurité.

8.4.1.2.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– démontrer l'efficacité des spécifications techniques de sécurité et veiller à ce que le mécanisme de sécurité ne puisse pas être contourné dans le mécanisme de mise en œuvre;

– mettre à jour la solution de sécurité dans les temps en cas de modification des exigences ou d'amélioration des technologies, jusqu'à ce que l'évaluation de la/des solution(s) soit achevée.

8.4.1.3 Évaluation de solutions

8.4.1.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– revoir régulièrement la proposition en matière de sécurité pour une infrastructure des mégadonnées, y compris l'architecture de sécurité et les fondements de la sécurité, tout en veillant à ce que les exigences de sécurité soient respectées.

8.4.1.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– établir un système d'évaluation de la sécurité et déterminer un ensemble de facteurs clés d'évaluation.

8.4.2 Construction de la sécurité

8.4.2.1 Architecture de sécurité

8.4.2.1.1 Exigences générales

Les fournisseurs BDSP doivent:

– établir une architecture de sécurité des services des mégadonnées et garantir la validité du processus d'élaboration et la réalisation des services de sécurité des mégadonnées décrits dans l'architecture de sécurité;

– veiller à ce que le domaine de sécurité décrit dans les documents sur l'architecture de sécurité soit conforme aux exigences relatives aux applications des mégadonnées et à l'architecture fonctionnelle de sécurité;

– veiller à ce que les documents sur l'architecture de sécurité décrivent un processus d'initialisation de la fonction de sécurité dans les applications des mégadonnées et l'infrastructure des mégadonnées, garantissant ainsi la sécurité de l'initialisation de la plate-forme et des applications.

8.4.2.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– veiller à ce que les informations reproduites dans les documents sur la description de l'architecture de sécurité soient suffisantes pour certifier que la fonction de sécurité des services des mégadonnées est en mesure de se protéger des altérations commises par des sujets qui ne sont pas dignes de confiance;
– veiller à ce que les documents sur la description de l'architecture de sécurité fournissent une analyse suffisante visant à prouver que le mécanisme de la fonction de sécurité des services des mégadonnées qui a été élaboré ne peut pas être contourné, et que les fonctions de sécurité qui sont proposées pour un système de mégadonnées ont été exécutées correctement.

8.4.2.2 Spécifications fonctionnelles

8.4.2.2.1 Exigences générales

Les fournisseurs BDSP doivent:

– fournir des spécifications fonctionnelles qui sont précises et complètes, et donner des précisions sur la correspondance entre les spécifications fonctionnelles et les exigences relatives à la fonction de sécurité des services des mégadonnées;
– veiller à ce que les spécifications fonctionnelles fournies décrivent intégralement les fonctions de sécurité des services des mégadonnées, et donner des précisions sur les relations dans la chaîne d'approvisionnement des données et les composantes de services en question;
– veiller à ce que les spécifications fonctionnelles fournies décrivent l'objectif de l'élaboration et la méthode d'emploi de toutes les interfaces d'application de la fonction de sécurité des services des mégadonnées et présentent tous les paramètres connexes des interfaces de la fonction de sécurité.

8.4.2.3 Déploiement de la sécurité

8.4.2.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– établir un processus de mise en œuvre de la sécurité pour la mise en œuvre de l'application des développeurs dans le système des services des mégadonnées;
– décrire la fonction de commande et les capacités relevant de chaque rôle des services des mégadonnées dans le processus de déploiement de la sécurité;
– décrire les fonctions et les interfaces disponibles pour chaque rôle des services des mégadonnées, indiquer une valeur de sécurité de manière appropriée, surtout pour tous les paramètres de sécurité contrôlés par les utilisateurs;
– décrire tous les rôles d'utilisateur des services des mégadonnées et veiller à ce que les politiques de sécurité décrites dans les politiques et spécifications de sécurité qui sont nécessaires pour gérer la sécurité de l'environnement soient suffisamment exécutées.

8.4.2.4 Protection aux limites

8.4.2.4.1 Exigences générales

Les fournisseurs BDSP doivent:

– définir le domaine de la sécurité et les limites de défense de la sécurité en harmonie avec le niveau de sécurité, y compris les politiques de contrôle de la sécurité et les politiques de gestion;
– définir le domaine de la sécurité et les limites de défense de la sécurité en ce qui concerne le contrôle opérationnel et l'isolement des applications, y compris les politiques de contrôle de la sécurité et les politiques de gestion;

– déployer les dispositifs de protection de la sécurité aux limites du domaine de la sécurité, pour détecter les incidents anormaux ou d'une éventuelle violation, et s'en protéger;
– adopter des mécanismes de défense de la sécurité stricts et comparatifs entre les domaines de sécurité, comme l'authentification de l'identité, la gestion des connexions, la politique de sécurité relative aux contrôles d'accès au réseau, la prévention des intrusions, le filtrage des informations et la vérification de l'intégrité des limites;
– élaborer une politique de gestion des mises à jour des dispositifs de défense de la sécurité et adopter les méthodes nécessaires pour garantir la mise en œuvre de la politique.

8.4.2.4.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– mettre en place des mesures et des mécanismes de protection personnalisée multi-locataires aux limites;
– définir un domaine ou sous-domaine de sécurité, un mécanisme d'isolement des données entre les domaines de sécurité et un mécanisme de contrôle d'accès pour les utilisateurs ou les rôles autorisés.

8.4.2.5 Gestion de documents

8.4.2.5.1 Exigences générales

Les fournisseurs BDSP doivent:

– dans un système des services des mégadonnées, mettre en œuvre une gestion des documents dont la portée inclut les stratégies, règles et politiques organisationnelles, les programmes des systèmes et les manuels de mise en œuvre;
– déterminer les processus de création, d'examen, d'approbation, de publication et d'archivage des documents, en précisant les responsabilités correspondantes en matière de sécurité dans chaque processus de gestion de documents;
– déterminer les exigences en termes de supports et de temps de stockage applicables aux documents, pour garantir leur disponibilité et leur exhaustivité;
– examiner régulièrement, mettre à jour, approuver et publier les documents, pour garantir que les utilisateurs sont informés des dernières versions;
– désigner les organismes responsables de l'établissement et du maintien du système de gestion des documents, et leur confier la responsabilité de la gestion des changements de version des documents;
– gérer la classification des documents de système.

8.4.2.5.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– créer une plate-forme pour gérer les documents au sein d'un fournisseur de services, en attribuant différentes permissions de visionnage en fonction des différents rôles;
– assurer la mise à jour et l'identification de la version nécessaires des documents correspondants lors de la mise à jour des produits ou services.

8.4.3 Opérations de sécurité

8.4.3.1 Gestion de la configuration des systèmes

8.4.3.1.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer et exécuter des procédures de gestion de la configuration des systèmes, établir une structure d'organisation de la gestion de la configuration des systèmes, préciser les rôles et les responsabilités des gestionnaires de la configuration, comme les administrateurs de systèmes, les opérateurs de systèmes, les responsables de la sécurité des systèmes, les auditeurs de systèmes, les administrateurs de bases de données et d'autres rôles;
– conformément aux exigences opérationnelles et aux objets de gestion, établir des processus d'approbation, d'opération et d'audit pour la gestion de la configuration, comme des éléments de configuration d'hôte, des éléments de configuration de réseau, des modules de service d'application et d'autres identifications de configuration de système, des configurations de contenus et des activités pertinentes liées au changement;
– conformément aux résultats des évaluations, établir une liste relative à la configuration de référence pour la fonction de sécurité des systèmes des mégadonnées et une liste de vérification quotidienne de la configuration, en réalisant la configuration nécessaire pour les fonctions de sécurité des systèmes des mégadonnées selon le principe du moindre privilège;
– conformément à l'accord de niveau de service des mégadonnées, configurer les paramètres des produits informatiques dans le système des mégadonnées, enregistrer et conserver les informations actuelles de configuration de la sécurité au sujet du système des mégadonnées;
– conformément aux stratégies d'utilisation, aux stratégies de restriction et aux politiques d'autorisation des logiciels achetés, interdire ou limiter l'utilisation par les logiciels d'un certain nombre de fonctions, ports, protocoles ou services du système des mégadonnées;
– donner des précisions sur une liste relative à la configuration contrôlée qui nécessite des changements réguliers, et mettre régulièrement à jour les éléments de configuration importants du système des mégadonnées en lien avec la sécurité de l'information, comme la base de données des virus, la base de données des règles applicables à la détection des intrusions, la base de données des règles applicables aux pare-feu et la base de données des vulnérabilités;
– examiner les changements apportés aux configurations contrôlées du système des mégadonnées, et les approuver ou les rejeter en fonction des résultats des analyses des incidences sur la sécurité, et consigner les décisions de changement;
– empêcher les développeurs et les intégrateurs de systèmes de changer directement le système des mégadonnées, le matériel pertinent, les logiciels et micrologiciels dans l'environnement de production, la configuration de l'audit et les événements de changement;
– avant de configurer ou d'apporter des modifications, tester, valider et enregistrer la configuration contrôlée et les éléments de changement, et analyser les éléments de changement du système pour estimer leurs incidences possibles sur la sécurité des services des mégadonnées;
– suivre les changements de paramètres de réglage de la configuration, et permettre de manière raisonnable l'exécution des fonctions de suivi, d'avertissement et de défense et d'autres fonctions des équipements de sécurité;
– prévoir des mesures d'intervention pertinentes pour faire face aux changements non autorisés, y compris des changements liés au personnel, la restauration d'une configuration établie ou l'interruption du fonctionnement d'un système d'information affecté dans des situations extrêmes.

8.4.3.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– effectuer une évaluation des risques des effets de la gestion de la configuration régulièrement, ou au moment où un changement important se produit dans l'architecture opérationnelle ou du système, réviser les exigences de configuration de base et les contenus de la configuration

conformément aux résultats de l'évaluation (par exemple, évaluer les risques et réviser les exigences de configuration au moins une fois par an);

– évaluer la stratégie d'évaluation des risques et ses effets régulièrement, ou au moment où un changement important se produit dans l'architecture opérationnelle ou du système; en fonction des résultats de l'évaluation, réviser les procédures de gestion de la configuration du système, ajuster la structure de gestion de l'organisation, configurer le processus de gestion, etc.;
– examiner régulièrement les configurations des systèmes des mégadonnées pour identifier les fonctions, ports, protocoles ou éléments de configuration de service non nécessaires ou non sécurisés;
– utiliser des outils de configuration de système ou des mécanismes automatiques pour la gestion centralisée, l'application et la vérification des paramètres des éléments de configuration;
– être en mesure de noter en temps réel les changements apportés aux infrastructures des mégadonnées et l'état des ressources virtuelles, avoir la possibilité d'ajuster automatiquement la configuration de la stratégie de sécurité des services de système.

8.4.3.2 Utilisation de services fournis par des tiers

8.4.3.2.1 Exigences générales

Les fournisseurs BDSP doivent:

– définir une politique de gestion de la sécurité pour les partenaires fournissant des services tiers;
– établir un mécanisme d'admission, d'évaluation et de notation pour les fournisseurs de services tiers;
– signer des accords de coopération relatifs aux composantes de service avec les fournisseurs de services tiers, préciser leurs obligations et leurs responsabilités (par exemple, éviter une trop grande implication des fournisseurs de services tiers dans les opérations de sécurité d'un système des mégadonnées);
– veiller à ce que les composantes de services tiers comprennent les mesures de sécurité de l'information du système des mégadonnées, appliquent correctement les mesures de sécurité requises et réussissent les tests des organismes d'évaluation des tiers;
– définir des politiques de sécurité relatives à l'emploi des composantes avec les fournisseurs de services tiers, préciser les conditions d'emploi et les possibilités d'accès des composantes externes;
– adopter les mesures techniques ou de gestion de la sécurité nécessaires pour veiller à ce que l'accès au système et aux ressources des données via les composantes de service externes soit autorisé et possible pour les utilisateurs des mégadonnées;
– effectuer un audit des informations, par exemple concernant les utilisateurs, les opérations actuelles et prévues des composantes de service externes, et garantir la traçabilité des services des mégadonnées.

8.4.3.2.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– évaluer les qualifications et les capacités de sécurité des fournisseurs de services tiers, et établir un mécanisme coopératif d'intervention en cas d'urgence avec les fournisseurs des composantes de service externes;

– veiller à ce que les composantes de service externes mettent en œuvre correctement les mesures de sécurité requises par la stratégie de sécurité de l'information et le plan de sécurité d'un système des mégadonnées, et réussissent le test des organismes d'évaluation des tiers;
– limiter l'utilisation de ressources de données sensibles dans les composantes de service externes par les membres du personnel autorisés, y compris les supports de stockage, les fichiers de données et d'autres ressources de données contrôlées par les fournisseurs BDSP.

8.4.3.3 Sécurité de la chaîne d'approvisionnement des technologies de l'information

8.4.3.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– définir des politiques et des procédures relatives à la sécurité de la chaîne d'approvisionnement des technologies de l'information, donner des précisions sur le mécanisme de filtrage, l'indice de filtrage et la méthode d'évaluation;
– donner des précisions sur les rôles et les opérations des participants à la chaîne d'approvisionnement des technologies de l'information en lien avec l'acquisition des données et les services de système;
– adopter les mesures techniques et de gestion nécessaires pour la substitution de la chaîne d'approvisionnement et garantir une intervention efficace en cas d'incident dans la chaîne d'approvisionnement.

8.4.3.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– établir un modèle de chaîne d'informations sur l'agrégation des données, y compris l'extraction des données, l'intégration et l'optimisation des sources de données de la chaîne d'approvisionnement;
– établir un mécanisme d'examen et d'évaluation pour la chaîne d'approvisionnement, effectuer régulièrement une évaluation des risques et une évaluation de la sécurité, par exemple au moins une fois par an;
– établir un mécanisme de gestion de la qualité de la chaîne d'approvisionnement des données et de retour d'information sur l'évaluation.

8.4.3.4 Gestion des correctifs de système

8.4.3.4.1 Exigences générales

Les fournisseurs BDSP doivent:

– définir des procédures de gestion des correctifs, concernant en particulier le téléchargement, les essais, l'analyse, la distribution, l'installation, l'archivage et d'autres processus et contenus, et assurer une gestion normalisée des correctifs de système;
– constituer une équipe de gestion des correctifs, suivre les informations sur la divulgation de vulnérabilités et les interventions en réponse aux événements de sécurité, télécharger, tester et installer des correctifs et effectuer d'autres tâches en suivant un programme approprié;
– établir un cadre de distribution et de gestion des correctifs de système, donner des précisions sur les mécanismes de téléchargement et de mise à jour des correctifs, comme la gestion des correctifs menée à la suite d'événements liés à la sécurité des systèmes, ou périodiquement à intervalles définis;
– disposer de capacités de test de la compatibilité des correctifs avant le déploiement et l'installation de correctifs, et relever les problèmes rencontrés durant les processus de mise à jour des correctifs;

– disposer de la fonction de vérification des correctifs et vérifier que les correctifs ont été installés avec succès.

8.4.3.4.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– établir un système de gestion des correctifs, mettre à jour le système et installer des correctifs via un logiciel.

8.4.3.5 Plan de continuité des activités

8.4.3.5.1 Exigences générales

Les fournisseurs BDSP doivent:

– évaluer régulièrement les risques liés aux activités en cours, et informer les utilisateurs sur les risques pertinents;

– élaborer et mettre en œuvre un plan approprié de sauvegarde en cas de sinistre conformément aux objectifs stratégiques organisationnels, en précisant le niveau de reprise, les impératifs liés à la reprise après sinistre et la stratégie de reprise des capacités du système après sinistre;

– effectuer régulièrement une analyse des incidences sur les activités et une évaluation des risques, et mettre en place une formation pertinente sur la continuité des activités.

8.4.3.5.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– effectuer régulièrement un test de commutation de système pour les infrastructures pertinentes des services des mégadonnées concernés, optimiser les programmes de sauvegarde des données et des ressources de système conformément aux exigences réelles;

– effectuer une simulation de plan de continuité des activités pour examiner l'intégrité, l'opérabilité et l'efficacité du plan de continuité des activités, vérifier la continuité des activités et la disponibilité des actifs de système.

8.4.4 Audit de sécurité

Les fournisseurs BDSP devraient mener à bien des audits de sécurité réguliers s'appliquant à l'ensemble de l'écosystème des services BDaaS. Un audit peut être effectué par une équipe d'audit interne indépendante ou des auditeurs tiers (agissant en tant que partenaires des services de mégadonnées (BDSN)). Les résultats des audits devraient être suffisamment visibles pour les utilisateurs des services de mégadonnées (BDSU).

8.4.4.1 Gestion de la stratégie d'audit

8.4.4.1.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer des stratégies et des procédures d'audit visant le comportement du système des mégadonnées et les activités relatives aux données des services des mégadonnées, y compris la cible de l'audit, l'objet de l'audit, l'exécution de l'audit, la méthode d'audit, la fréquence d'audit, les rôles et responsabilités pertinents, l'engagement de la direction, la coordination des participants à la chaîne d'approvisionnement et l'analyse de conformité;

– élaborer un processus de gestion des changements pour les stratégies et procédures d'audit, enregistrer en détail l'état d'avancement des stratégies et procédures d'audit, de la politique d'exécution des changements, de la description des changements, etc., examiner et mettre à jour régulièrement les stratégies et procédures d'audit;

– donner des précisions sur les privilèges et les responsabilités des utilisateurs dans le cadre des stratégies et procédures d'audit, définir une procédure pertinente d'octroi de privilèges dans le cadre des stratégies et procédures d'audit, et les rôles en matière d'exécution de la stratégie d'audit et de gestion des données d'audit.

8.4.4.1.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– établir des procédures d'audit de la sécurité de la chaîne d'approvisionnement des données et des mécanismes de coordination, et veiller à la traçabilité des événements d'audit;

– vérifier et évaluer régulièrement la mise en œuvre des stratégies et procédures d'audit;

– créer des postes d'auditeurs indépendants dans le domaine de la sécurité des systèmes, qui devraient mener des audits de sécurité réguliers concernant les services des mégadonnées;

– disposer de technologies et d'outils d'analyse de la conformité pour les stratégies et procédures d'audit basées sur les données d'audit.

8.4.4.2 Génération de données d'audit

8.4.4.2.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer une réglementation relative à l'enregistrement des données d'audit, et donner des précisions sur la structure et le format organisationnels des données d'audit;

– préciser les événements pouvant faire l'objet d'un audit liés aux actions du système des mégadonnées, par exemple la connexion de l'utilisateur, la gestion de compte, l'accès invité, le changement de stratégie, l'autorisation d'accéder à une fonctionnalité privilégiée ou la mise à jour de module de service;

– préciser les événements pouvant faire l'objet d'un audit liés aux activités relatives aux données des services des mégadonnées, par exemple la collecte de données, l'accès aux données, le stockage de données, le transfert de données, le traitement de données, la conservation de données et la destruction de données;

– veiller à ce que les données d'audit enregistrées incluent au moins la durée de l'opération, le thème de l'opération, le type d'opération, l'objet de l'opération et les résultats de l'opération;

– disposer de capacités d'audit à granularité fine pour l'exploitation des données et les actions concernant les services de système;

– disposer d'une marque horaire fiable pour l'enregistrement d'audit. La granularité temporelle devrait être conforme aux exigences en matière d'audit;

– disposer des capacités de sélectionner et d'examiner les événements pouvant faire l'objet d'un audit;

– tenir régulièrement à jour les politiques d'enregistrement des données, les événements pouvant faire l'objet d'un audit et les enregistrements d'audit.

8.4.4.2.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– fournir des interfaces de système pour l'accès aux données d'audit des tiers;

– adopter des technologies de cryptographie pour garantir la non-répudiation des données d'audit.

8.4.4.3 Protection des données d'audit

8.4.4.3.1 Exigences générales

Les fournisseurs BDSP doivent:

– mettre en place des méthodes et des mécanismes de gestion de la sécurité du stockage persistant de grandes quantités de données d'audit;

– disposer des capacités d'autoriser l'accès aux données d'audit, et autoriser l'accès aux données d'audit à des administrateurs d'audit déterminés;

– adopter des technologies de sécurité ou des mesures de contrôle pour garantir l'authenticité des données d'audit;

– fournir une fonctionnalité d'archivage des données d'audit, et favoriser des méthodes et des mécanismes de chiffrement hors ligne pour le stockage de données d'audit;

– établir des stratégies et des méthodes de gestion pour un stockage efficace des données d'audit, la compression des données, etc.;

– améliorer la gestion de l'accès aux données d'audit, et enregistrer toutes les opérations concernant les données d'audit;

– disposer d'une capacité de désensibilisation pour les données d'audit exportées;

– veiller à l'efficacité de l'enregistrement d'audit stocké si les capacités de stockage d'audit sont épuisées, invalidées ou font l'objet d'une attaque.

8.4.4.3.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– disposer de capacités de reprise après sinistre à distance et de sauvegarde;

– être en mesure de fournir des éléments de preuve pour démontrer l'authenticité et l'exhaustivité des données d'audit fournies.

8.4.4.4 Rapport d'analyse d'audit

8.4.4.4.1 Exigences générales

Les fournisseurs BDSP doivent:

– élaborer des stratégies et des procédures d'audit, d'analyse et de rapport applicables aux enregistrements d'audit;

– examiner et analyser les enregistrements d'audit régulièrement, et élaborer un rapport d'analyse d'audit;

– distribuer un rapport d'analyse aux responsables désignés du personnel d'une organisation. Si tout risque majeur pour la sécurité ou comportement illicite est découvert pendant l'audit, faire rapport aux responsables de l'organisation dès que possible.

8.4.4.4.2 Exigences renforcées

Les fournisseurs BDSP devraient:

– suivre et analyser les événements pouvant faire l'objet d'un audit en temps réel, pour appuyer le suivi des actions suspectes et les interventions en réponse à ces actions;

– disposer de capacités d'analyse de corrélation des enregistrements d'audit de sources différentes.

Bibliographie

[b-UIT-T M.3030] Recommandation UIT-T M.3030 (2002), *Langage de balisage pour les télécommunications (tML): cadre général.*

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

[b-UIT-T Y.3602] Recommandation UIT-T Y.3602 (2018), *Mégadonnées – Exigences fonctionnelles relatives à la provenance des données.*

[b-NIST SP 800-30] Publication spéciale du NIST SP 800-30 (2012), *Guide pour l'évaluation des risques*.

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	Équipements 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, 2021