Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1751

(09/2020)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de datos – Seguridad de los macrodatos

Directrices de seguridad para la gestión del ciclo de vida de los macrodatos por los operadores de telecomunicaciones

Recomendación UIT-T X.1751

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	**X.1750–X.1759**
SEGURIDAD DE 5G	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1751

Directrices de seguridad para la gestión del ciclo de vida de los macrodatos por los operadores de telecomunicaciones

Resumen

En la Recomendación UIT-T X.1751 se analizan vulnerabilidades de seguridad y se proporcionan directrices de seguridad para la gestión del ciclo de vida de los macrodatos por los operadores de telecomunicaciones.

Con la rápida velocidad a la que evoluciona la tecnología de macrodatos, el valor de los datos ha aumentado considerablemente. Los macrodatos brindan nuevas oportunidades a los servicios de telecomunicaciones. Anteriormente, los datos se almacenaban y gestionaban de manera aislada e independiente en diferentes sistemas de servicios de telecomunicaciones. La tendencia a la combinación y fusión de datos son inevitables con la aparición de los servicios de macrodatos. En el proceso de convergencia y fusión de datos, los datos fluyen a través de plataformas y procesos de servicio. Surgen así diversas vulnerabilidades de seguridad en las diferentes etapas del ciclo de vida de los datos.

En la Recomendación UIT-T X.1751 se presentan características específicas de los servicios de macrodatos y categorías de datos en el ámbito de las telecomunicaciones, se analizan vulnerabilidades de seguridad propias de la gestión del ciclo de vida de los macrodatos y se especifican directrices de seguridad para los operadores de telecomunicaciones.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1751	2020-09-03	17	11.1002/1000/14267

Palabras clave

Gestión del ciclo de vida de los datos, servicios de macrodatos de telecomunicaciones.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1751

Directrices de seguridad para la gestión del ciclo de vida de los macrodatos por los operadores de telecomunicaciones

1 Alcance

En esta Recomendación se describen las vulnerabilidades de seguridad y se establecen directrices de gestión del ciclo de vida para los servicios de macrodatos de telecomunicaciones. Esta Recomendación:

– presenta las características de los servicios de macrodatos de telecomunicaciones y categorías de datos;

– analiza las vulnerabilidades de seguridad de la gestión del ciclo de vida para los servicios de macrodatos de telecomunicaciones;

– especifica directrices de seguridad para la gestión del ciclo de vida de los servicios de macrodatos de telecomunicaciones.

Cuando los operadores de telecomunicaciones prestan servicios de macrodatos, el prerrequisito básico es que se haya obtenido el consentimiento explícito de los abonados. Además, en el caso de los operadores de telecomunicaciones, se recomienda adoptar las medidas de protección de datos necesarias durante todo el proceso de servicios de macrodatos.

Los mecanismos de protección para las diversas categorías de datos quedan fuera del alcance de la presente Recomendación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación

[ITU-T X.1641] Recomendación ITU-T X.1641 (2016), *Directrices para la seguridad de los datos de cliente de los servicios en la nube.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 macrodatos [b-ITU-T Y.3600]: Paradigma que permite la recopilación, el almacenamiento, la gestión, el análisis y la visualización, potencialmente en condiciones de tiempo real, de grandes volúmenes de datos con características heterogéneas.

3.1.2 macrodatos como servicio (BDaaS) [b-ITU-T Y.3600]: Categoría de servicio en la nube en la que las capacidades que se ponen a disposición del cliente del servicio en la nube le permiten recopilar, almacenar, analizar, visualizar y gestionar los datos utilizando macrodatos.

3.1.3 capacidad de vinculación [b-ISO/IEC 20889]: Propiedad de un conjunto de datos, que permite asociar (mediante un vínculo) un registro relativo a una entidad principal de datos con otro registro relativo a la misma entidad principal de datos en un conjunto de datos distinto.

3.1.4 pseudoanonimización [b-ISO/IEC 29100]: Proceso aplicable a la información de identificación personal (PII) mediante el cual se sustituye la información de identificación por un alias.

3.1.5 política de seguridad [b-ITU-T X.800]: Conjunto de criterios para la prestación de servicios de seguridad.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 ciclo de vida de los datos: Todo el proceso de supervivencia después de que se generan, comprendida su recopilación, transmisión, almacenamiento, utilización (que comprende su análisis y visualización), intercambio y destrucción.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

2B	para empresas
2C	para el consumidor
API	Interfaz de programación de aplicaciones
APP	Aplicación
BDaaS	Macrodatos como servicio
BSS/OSS	Sistema de apoyo corporativo y sistema de apoyo operativo
DB	Base de datos
FTP	Protocolo de transferencia de ficheros
HDFS	Sistema de ficheros distribuido Hadoop
IoT	Internet de las cosas
IP	Protocolo Internet
JDBC	Conectividad a bases de datos Java
LBS	Servicios basados en la ubicación
LDAP	Protocolo ligero de acceso al directorio
MPP	Procesador en paralelo masivo
OSS	Sistema de apoyo operativo
PII	Información de identificación personal
REST	Transferencia de estado representativo

5 Convenios

En esta Recomendación:

La expresión **"se requiere"** indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

La expresión **"se recomienda"** indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión **"se prohíbe"** indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

La expresión **"puede opcionalmente"** indica que el requisito se permite, sin que ello signifique que se recomienda. La expresión no implica que el fabricante deba ofrecer esta opción, ni que el operador de red o de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esa funcionalidad sin que ello afecte a la conformidad con la presente Recomendación.

6 Generalidades

De resultas de su rápido desarrollo, el valor de los macrodatos ha aumentado considerablemente. Los macrodatos brindan nuevas oportunidades a los operadores de telecomunicaciones, que han dispuesto durante mucho tiempo de diferentes tipos de recursos de datos, como datos de llamadas, de localización, personales, de consumidores móviles y de terminales, en lo que se han denominado centrales de almacenamiento de datos. Dada la rapidez a la que se generan macrodatos, los operadores de telecomunicaciones están constantemente innovando e invirtiendo en el desarrollo de servicios de macrodatos.

Los servicios de datos de telecomunicaciones generan volúmenes de información del orden de terabytes o incluso petabytes. Los datos generados son de diversos tipos, a saber, estructurados, semiestructurados y no estructurados. Las fuentes incluyen datos privados, como información de identificación personal (PII), y datos del registro de accesos. Esos datos pueden ser objeto de ataques.

Anteriormente, los datos se separaban y gestionaban de manera independiente en diferentes sistemas de servicios de telecomunicaciones. Además, esos sistemas podían estar situados en diversos emplazamientos y ser administrados por diferentes departamentos. Con el desarrollo de los servicios de macrodatos, los operadores de telecomunicaciones están eliminando la separación departamental y recabando datos de varios sistemas separados. La convergencia de datos aumenta sobremanera el valor de los servicios de macrodatos.

En un proceso de servicio de macrodatos, los datos fluyen a través de la plataforma de macrodatos y pasan por varias etapas del ciclo de vida, en cada una de las cuales la información se ve expuesta a diversas amenazas y riesgos de seguridad. Por ejemplo, una recopilación de datos inadecuada puede dar lugar a una divulgación de información improcedente. En la etapa de almacenamiento de datos puede producirse un acceso no autorizado. La utilización de datos confidenciales puede crear el riesgo de filtración de datos cuando se comparte información. Por lo tanto, es necesario analizar vulnerabilidades de seguridad y especificar las directrices de seguridad para la gestión del ciclo de vida en los servicios de macrodatos de telecomunicaciones.

En esta Recomendación se analizan los riesgos de seguridad y se especifican directrices de seguridad para la gestión del ciclo de vida de macrodatos de telecomunicaciones.

7 Características de los servicios de macrodatos de telecomunicaciones y categorías de datos

7.1 Características de los servicios de macrodatos de telecomunicaciones

Cada vez son más los operadores de telecomunicaciones que están adoptando servicios de macrodatos como importante dirección estratégica para la innovación y el desarrollo de sus empresas. Por ejemplo, mediante la construcción de plataformas con capacidad de macrodatos o la creación de

equipos operativos especializados, los operadores de telecomunicaciones pueden desarrollar servicios de macrodatos.

Los operadores de telecomunicaciones pueden recopilar ingentes volúmenes de datos de cliente sobre un usuario determinado, como el perfil del usuario, los dispositivos, la utilización y la ubicación. Los operadores de telecomunicaciones pueden utilizar técnicas de análisis de macrodatos para, a partir de esos datos, desarrollar servicios relacionados con una amplia variedad de aplicaciones, por ejemplo, el comercio minorista, la atención sanitaria y las ciudades inteligentes. Los operadores de telecomunicaciones pueden utilizar estos servicios para mejorar sus propios negocios o venderlos a terceros que ofrecen servicios en otros sectores empresariales.

Sin embargo, la magnitud y los tipos de datos que los operadores de telecomunicaciones utilizan para estos servicios de macrodatos permiten revelar una asombrosa cantidad de detalles sobre las personas, incluida la PII, datos sensibles, por ejemplo, creencias religiosas o afiliaciones políticas, y secretos comerciales. Resulta especialmente importante que los operadores de telecomunicaciones tomen esto en consideración si deciden compartir estos datos con terceros. Por consiguiente, resulta esencial que los operadores de telecomunicaciones reconozcan las amenazas durante el ciclo de vida de los servicios de macrodatos y adopten medidas de seguridad para proteger a sus usuarios.

7.2 Categorías de datos

Los operadores de telecomunicaciones disponen de cuatro categorías principales de datos de usuarios, que se enumeran a continuación. Además, con el desarrollo de la Internet de las cosas (IoT) y sus servicios, la profundidad y amplitud de los datos no dejan de aumentar. Esta expansión conlleva nuevos riesgos para la confianza y la seguridad de los usuarios, que deben resolver los operadores de telecomunicaciones, con respecto a:

1) los datos generados por el sistema de apoyo corporativo y el sistema de apoyo operativo (BSS/OSS) del operador de telecomunicaciones, que consisten en la identidad del usuario, la duración de la llamada, el destinatario de la llamada, la factura de la comunicación, los tipos de servicio e incluso el tipo de terminal;
2) los datos generados por el sistema de apoyo operativo (SSO) del operador de telecomunicaciones, que son principalmente datos sobre el comportamiento del usuario, incluidos los generados a través de Internet móvil, charlas, juegos y navegación por la web;
3) datos dimanantes de la información del servicio basado en la ubicación del usuario (SBL), que, a diferencia de las categorías 1) y 2), están estrechamente relacionados con la ubicación real del usuario y pueden utilizarse para la publicidad comercial, la movilidad de la población, la seguridad pública y la planificación urbana;
4) datos para empresas (2B) o para consumidores (2C), generados en contextos de IoT que giran en torno a macrodatos sobre "cosas" y "personas", que son de gran valor en los ámbitos de la atención sanitaria, los dispositivos de bolsillo y los hogares inteligentes.

Los macrodatos sobre las cosas incluyen: consumo de agua, electricidad y gas registrados en los contadores; datos sobre el clima y la contaminación recogidos mediante sensores; y datos de rastreo sobre los envíos de bienes.

Los macrodatos sobre las personas incluyen: datos sobre la salud, finanzas personales y el historial de compras.

Obsérvese que la posibilidad de vincular ciertos datos puede tener mayores consecuencias sobre los usuarios de lo esperado, según la forma en que se clasifiquen inicialmente los datos; por ejemplo, los datos anonimizados de categoría 4) que se analizan junto con otros datos pueden, no obstante, hacer identificables a las personas, como PII de categoría 1). Por consiguiente, se recomienda que la posibilidad de establecer vínculos sea un aspecto fundamental a la hora de determinar la forma de proteger los datos, incluso en los casos en que éstos no se clasifiquen inmediatamente como PII u otros datos personales.

En la presente Recomendación, se recomienda velar por la seguridad de los datos de estas cuatro categorías en todas las etapas del ciclo de vida de los datos mediante directrices de seguridad.

8 Ciclo de vida de los datos en los servicios de macrodatos de telecomunicaciones

El ciclo de vida útil de los datos relativos a los servicios de macrodatos de telecomunicaciones consta de seis etapas principales: recopilación; transmisión; almacenamiento; utilización; compartición; y destrucción. La etapa de transmisión de datos puede constar de varias fases.

En la Figura 1 se ilustra el ciclo de vida de los datos en los servicios de macrodatos de telecomunicaciones.

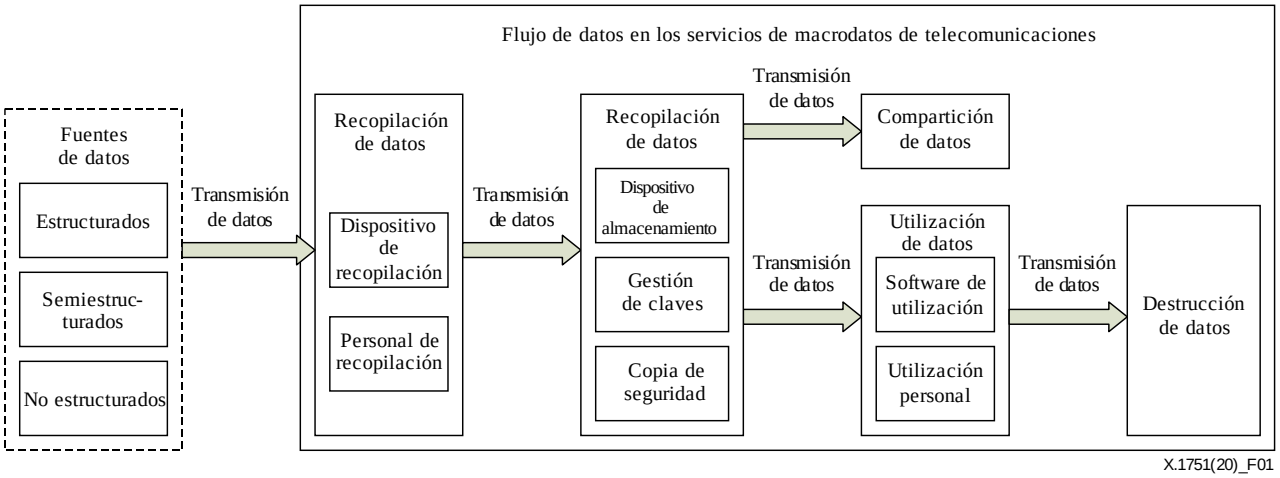

Figura 1 – Ciclo de vida de los datos en los servicios de macrodatos de telecomunicaciones

El ciclo de vida de los servicios de macrodatos de telecomunicaciones comienza con la recopilación de datos y termina con su destrucción. Después de la recopilación, los datos se pueden transmitir, almacenar, utilizar y compartir. La transmisión de los datos puede efectuarse en diferentes etapas, por ejemplo, una vez recopilados, los datos pueden transmitirse a dispositivos de almacenamiento especializados; durante su utilización, los datos pueden transmitirse de los dispositivos de almacenamiento al software o entidad para su utilización; después de utilizados, los datos que han expirado o resultan inútiles se destruyen.

Recopilación de datos: mediante dispositivos o entidades especializados de recopilación de datos, se recopilan diferentes tipos y categorías de datos para su almacenamiento en un directorio específico o en un directorio temporal.

Transmisión de datos: este proceso implica la transferencia de datos desde un dispositivo de recopilación a un dispositivo de almacenamiento y desde éste la transferencia para su utilización y compartición. A veces la etapa de destrucción de datos conlleva también la transmisión de datos.

Almacenamiento de datos: los datos se almacenan en dispositivos previstos para tal fin, por ejemplo, en bases de datos (DB), sistemas de archivos distribuidos y matrices de discos. La encriptación y la copia de seguridad de los datos también son necesarios para los datos importantes.

Utilización de los datos: el software y las aplicaciones de análisis de datos acceden a los datos y los procesan para proporcionar diversos servicios de macrodatos. Este proceso puede incluir diversos datos personales sensibles.

Compartición de datos: el proveedor de servicios de datos o el propietario de dichos datos comparte los resultados de su procesamiento de análisis de datos o incluso los datos de origen con otros proveedores o con terceros.

Destrucción de datos: los datos expirados, especialmente los que se encuentran en dispositivos que almacenan información importante o sensible, se deben destruir completamente mediante un mecanismo de seguridad previsto para tal fin.

9 Vulnerabilidades de seguridad en el ciclo de vida de los servicios de macrodatos de telecomunicaciones

En el proceso de los servicios de macrodatos de telecomunicaciones, los datos fluyen en cada paso del servicio. Las vulnerabilidades de seguridad pueden surgir desde dentro o fuera del proceso. Las vulnerabilidades de seguridad internas están relacionadas con distintos dispositivos y sistemas, como los de recopilación, almacenamiento y utilización. Las vulnerabilidades de seguridad externas se producen debido a una mala configuración o al uso indebido. Las vulnerabilidades relacionadas con los datos se describen en [b-ITU-T X.1040].

9.1 Etapa de recopilación de datos

9.1.1 Vulnerabilidad de seguridad en dispositivos y sistemas

Los dispositivos y sistemas son vulnerables y pueden estar infectados por virus o troyanos, causando problemas de seguridad.

9.1.2 Vulnerabilidad de seguridad en la configuración y gestión

1) Gestión personal

Los dispositivos de recopilación de datos pueden utilizarse de manera inadecuada o sin autorización, generando un riesgo de filtración de datos.

2) Gestión del dispositivo

La configuración errónea o perniciosa de los dispositivos de recopilación pueden dar lugar a la recopilación no autorizada y a la filtración de datos.

Los datos se recaban mediante distintos sistemas empresariales situados en emplazamientos distintos y gestionados por diferentes departamentos. Un nodo pernicioso puede penetrar en el sistema de dispositivos para realizar operaciones no autorizadas de recopilación de datos.

3) Gestión de los datos

Se recopilan más datos de los necesarios para los fines previstos, lo que puede dar lugar a una filtración de datos.

Durante la etapa de recopilación, una zona de almacenamiento temporal de datos, como un trayecto aleatorio del servidor de protocolo de transferencia de ficheros (FTP), escapa al control del personal de recopilación, aumentando así el riesgo de divulgación de datos o de alteración no autorizada.

9.2 Etapa de transmisión de datos

9.2.1 Vulnerabilidad de seguridad en la configuración y gestión

1) Gestión personal

El administrador modifica el puerto de transmisión o la configuración de transmisión sin autorización, lo que puede producir una filtración de datos.

2) Gestión del dispositivo

Los datos recopilados se transmiten por un canal inseguro, haciendo a los datos susceptibles de ser leídos o alterados.

La interfaz de transmisión no está autenticada, produciéndose una conexión errónea o perniciosa.

El mecanismo de transmisión entre diferentes nodos no protege la confidencialidad e integridad de los datos, dando lugar a filtraciones de datos y aumentando el riesgo de alteración, lectura e interceptación.

3) Gestión de los datos

La falta de protección de la confidencialidad durante la transmisión de los datos puede dar lugar a la interceptación o la filtración de datos.

La falta de protección de la integridad durante la transmisión de datos puede dar lugar a la manipulación perniciosa o al deterioro de los datos.

La falta de protección de la disponibilidad durante la transmisión puede dar lugar a la interceptación o la alteración de los datos.

9.3 Etapa de almacenamiento de datos

9.3.1 Vulnerabilidad de seguridad en dispositivos y sistemas

La no utilización de ningún software antivirus o de un software de seguridad expirado causa la divulgación y alteración de datos sensibles.

La falta de mantenimiento o la mala configuración del software de seguridad deja los datos sin protección, lo que puede dar lugar a la divulgación y alteración de los datos y a ataques contra los mismos.

9.3.2 Vulnerabilidad de seguridad en la configuración y la gestión

1) Gestión personal

Las medidas de control de acceso están incorrectamente configuradas de manera que los datos almacenados están en riesgo de acceso o alteración no autorizados. Las personas autorizadas a acceder a determinados conjuntos de datos almacenados pueden deducir cierta información personal u otros datos personales a los que no están autorizadas, debido a la posibilidad de vinculación.

2) Gestión del dispositivo

En un entorno de almacenamiento, existen a la vez una DB relacional, un sistema de archivos distribuidos Hadoop (HDFS) y un centro de datos con procesador paralelo masivo (MPP). Una gestión deficiente de los permisos puede dar lugar a accesos no autorizados y a la divulgación de datos.

Muchos datos no estructurados se almacenan por separado en distintos nodos, lo que dificulta la aplicación de la misma política de seguridad. Las políticas de seguridad incoherentes o contradictorias pueden menoscabar la protección de seguridad y causar filtración de datos.

3) Gestión de los datos

Los datos almacenados no están total o parcialmente encriptados, aumentan así la exposición de los usuarios en caso de que se produzca una filtración pasiva o activa de los datos.

Los datos almacenados están encriptados; sin embargo, las vulnerabilidades relacionadas con el algoritmo de encriptación o la gestión de claves aumentan el riesgo de acceso no autorizado a los datos almacenados o su alteración.

La integridad de los datos no se protege activamente durante su almacenamiento, exponiéndolos a una modificación no autorizada incluso después de su recopilación.

Los datos almacenados incluyen datos desactualizados o que no son directamente pertinentes y necesarios para los fines previstos. A medida que aumenta el número de datos almacenados, también aumenta la exposición del usuario en caso de cualquier filtración pasiva o activa de los datos.

Las copias de seguridad y o los mecanismos de recuperación de datos incompletos pueden dar lugar a la pérdida de datos.

9.4 Etapa de utilización de los datos

9.4.1 Vulnerabilidad de seguridad en dispositivos y sistemas

El software de análisis de datos que está en red o en la nube tiene vulnerabilidades que ponen en riesgo los datos expuestos al software.

La aplicación de visualización del software de análisis de datos tiene problemas de seguridad que pueden ser explotados por los atacantes.

9.4.2 Vulnerabilidad de seguridad en la configuración y gestión

1) Gestión del personal

Si no existen capacidades de autenticación y autorización de usuarios o aplicaciones de visualización, un usuario o una aplicación de visualización falsa puede obtener datos visuales, produciéndose una filtración de datos.

2) Gestión del dispositivo

La falta de autenticación de la identidad en los dispositivos que utilizan datos da lugar a que dispositivos no autorizados se incorporen a la gran plataforma de datos. En consecuencia, se produce una filtración de datos o indisponibilidad para la empresa.

3) Gestión de datos

Cuando se utilizan mediante aplicaciones de visualización, los datos personales, incluida la PII y los datos sensibles, no se anonimizan o enmascaran adecuadamente, aumentando así las posibilidades de identificación.

Los datos visualizados son altamente vinculables, lo que aumenta las posibilidades de inferir la identidad u otros datos personales.

Los datos resultantes de los procesos de análisis de datos no se almacenan en un entorno seguro, o se conservan datos desactualizados o que no son directamente pertinentes o necesarios para los fines previstos. Cuantos más datos se conserven, mayor será la exposición del usuario en caso de producirse una filtración pasiva o activa de los datos.

Los registros de datos producidos durante esta etapa no se almacenan de forma segura, pudiéndose utilizar para deducir datos personales en caso de filtración de datos.

9.5 Etapa de compartición de datos

9.5.1 Vulnerabilidad de seguridad de dispositivos y sistemas

Los dispositivos y sistemas de compartición de datos son vulnerables o están infectados por virus o troyanos, causando problemas de seguridad.

9.5.2 Vulnerabilidad de seguridad en la configuración y la gestión

1) Gestión del personal

Las responsabilidades y capacidades de seguridad de los usuarios de los datos compartidos no se especifican adecuadamente, lo que da lugar a una protección de datos inadecuada y a la filtración de datos.

2) Gestión del dispositivo

El alcance y los límites de la compartición de datos no están claramente definidos; además, faltan medidas de control de la seguridad, exponiendo directamente los datos delicados a los asociados.

El canal de compartición de datos carece de protección de seguridad, lo que da lugar a la divulgación o la manipulación de datos importantes.

3) Gestión de datos

Los registros de registro de compartición de datos están incompletos, lo que dificulta la determinación de la causa una vez que se produce un incidente de seguridad.

9.6 Etapa de destrucción de datos

Al final de esta etapa, si los datos no se han destruido totalmente, el personal malintencionado podría recuperar datos sensibles, dando lugar a una filtración de datos.

9.7 Relación entre la vulnerabilidad de seguridad y el ciclo de vida de los datos

Las vulnerabilidades de seguridad aparecen en diferentes etapas del ciclo de vida de un servicio de macrodatos. En el Cuadro 1 se muestra una descripción general de la relación entre la vulnerabilidad de seguridad y el ciclo de vida de los datos de un servicio de macrodatos.

En el Cuadro 1, la letra "S" (Sí) indica que existe una vulnerabilidad de seguridad en esa etapa.

Cuadro 1 – Relación entre la vulnerabilidad de seguridad y la etapa del ciclo de vida de los datos

Vulnerabilidad		Etapa del ciclo de vida					
		Recopilación	**Transmisión**	**Almacenamiento**	**Utilización**	**Comparación**	**Destrucción**
Vulnerabilidad en el dispositivo		S		S	S	S	
Vulnerabilidad en la configuración y gestión	Gestión del personal	S	S	S	S	S	
	Gestión del dispositivo	S	S	S	S	S	
	Gestión de los datos	S	S	S	S	S	S

10 Directrices de seguridad sobre el ciclo de vida de los datos de los servicios de macrodatos de telecomunicaciones

En esta Recomendación se describen en detalle mecanismos que resultan adecuados para todas las categorías de datos descritos en la cláusula 7.2.

10.1 Etapa de recopilación de datos

10.1.1 Directrices de seguridad para dispositivos y sistemas

Se requiere que el software del dispositivo y del sistema utilizado para recopilar datos esté actualizados y no tenga vulnerabilidades públicas.

Se requiere que los dispositivos y sistemas utilizados para recopilar datos tengan instalado software de seguridad, como antivirus y anti-malware, compatible con el sistema operativo del dispositivo.

10.1.2 Directrices de seguridad para la configuración y gestión

1) Gestión del personal

Se recomienda informar a los usuarios sobre qué datos se recaban y cómo, y obtener su consentimiento explícito antes de comenzar la recopilación.

Al realizar la recopilación de datos, es necesaria la autentificación y la autorización del personal de recopilación.

2) Gestión del dispositivo

Se recomienda especificar mecanismos de seguridad y medidas de protección para la recopilación de datos, por ejemplo, a efectos de una autenticación y una autorización estrictas de los dispositivos empleados para la recopilación. Se recomienda categorizar los datos para cumplir con los principios recopilación.

Se requiere configurar un servicio de macrodatos para cumplir con la finalidad de servicio prevista. Se requiere determinar los datos cuya recopilación resulta estrictamente pertinente y necesaria para los fines previstos.

Se requiere especificar el dispositivo de recopilación de datos, los canales de recopilación, los formatos de datos, los procesos de recopilación y los métodos utilizados.

Se requiere aplicar la autenticación del acceso al dispositivo y al personal de recopilación; se requiere detectar y advertir de cualquier comportamiento de recopilación anómalo.

Se requiere que la zona de almacenamiento temporal esté estrictamente restringida, por ejemplo, mediante la prohibición de las exportaciones de datos no autorizadas desde dichas zonas hasta otros recursos de almacenamiento, y se recomienda que toda modificación de la zona de almacenamiento esté sujeta a autorización.

Se recomienda proteger la transmisión de los datos recopilados, metadatos inclusive, mediante algoritmos de encriptación ampliamente utilizados y de eficacia probada por terceros fiables.

Gestionar y almacenar con seguridad las claves de encriptación y, en la medida de lo posible, dar preferencia a los protocolos criptográficos con función de secreto permanente.

3) Gestión de datos

En función de su importancia y sensibilidad, se recomienda determinar las distintas clasificaciones de los datos recopilados.

Se requiere recurrir a registros de actividad y alertas cuando se detecte comportamiento anómalo, como el siguiente:

- la recopilación y transmisión reiteradas rebase el umbral determinado;
- la transmisión se interrumpe durante el proceso de recopilación;
- se rebasa el umbral de capacidad establecido.

10.2 Etapa de transmisión de datos

10.2.1 Directrices de seguridad para la configuración y gestión

1) Gestión del personal

Impedir a los administradores modificar arbitrariamente el puerto de transmisión o los parámetros de configuración de la interfaz.

2) Gestión del dispositivo

Se requiere la transmisión de datos por un canal encriptado de extremo a extremo.

La interfaz de transporte proporciona capacidades de encriptación para impedir que se produzcan conexiones perniciosas.

3) Gestión de datos

Se recomienda proteger la confidencialidad e integridad de los datos en la etapa de transmisión.

Se recomienda detectar sin dilación cualquier daño a la integridad de los datos durante la transmisión y tomar las medidas necesarias para restablecerlos después de detectar los errores.

10.3 Etapa de almacenamiento de datos

10.3.1 Directrices de seguridad para dispositivos y sistemas

Se requiere mantener actualizado el software del dispositivo y del sistema de almacenamiento y que no presenten vulnerabilidades públicas.

Se requiere que el dispositivo de almacenamiento tenga instalado software de seguridad actualizado.

10.3.2 Directrices de seguridad para la configuración y gestión

1) Gestión del personal

Se requiere aplicar un método de control de acceso para usuarios o aplicaciones, como el protocolo de autenticación de red de clave secreta, Kerberos o la autorización específica.

Se recomienda integrar las operaciones de datos importantes en el modo de control de bóveda de operaciones multipartitas, de modo que una sola persona no pueda tener plena autoridad operativa para los datos importantes, como obtención por lotes, copia, destrucción, publicación y utilización.

2) Gestión del dispositivo

Los métodos de autorización deben permitir el acceso exclusivamente a las personas que son esenciales para realizar los fines para los que se recopilan datos. Deben establecerse permisos para impedir el acceso de las personas a datos distintos de los indispensables para el ejercicio de sus funciones específicas y tener en cuenta la posibilidad de deducir datos personales mediante la vinculación entre los conjuntos de datos almacenados y los permisos separados entre las personas.

3) Gestión de datos

a) Minimización de datos

Se recomienda restringir el almacenamiento de datos, incluidos los resultados de los procesos realizados durante la etapa de utilización de los datos, de modo que sólo se conserven los datos que sean pertinentes y necesarios para el propósito declarado de utilización.

Se recomienda establecer periodos máximos de retención claros para todos los datos, basados en el mínimo tiempo posible que deben retenerse los datos para cumplir los fines previstos.

b) Almacenamiento de datos encriptados

El almacenamiento encriptado es necesario para garantizar la confidencialidad de los datos importantes. Se recomienda emplear un modelo jerárquico de encriptado de datos; se utilizan diferentes mecanismos de almacenamiento de seguridad en función del grado de confidencialidad de los datos.

Se recomienda recurrir a algoritmos de encriptado ampliamente utilizados y de eficacia probada por terceros fiables. Gestionar y almacenar con seguridad las claves de encriptación y, en la medida de lo posible, dar preferencia a los protocolos criptográficos con función de secreto permanente.

c) Protección de la integridad de los datos

Se recomienda proporcionar un mecanismo de detección de la integridad para determinar los daños y pérdidas de datos debido al almacenamiento de los mismos.

Se recomienda tomar las medidas necesarias para restaurar la integridad de los datos cuando se detecten errores [UIT-T X.1641].

Deben mantenerse registros de auditoría que documenten cualquier alteración de los datos almacenados. Los registros deben almacenarse de manera segura y se recomienda registrar e informar de cualquier intento de alteración.

d) Copia de seguridad y recuperación de datos

Se recomienda proporcionar mecanismos de copia de seguridad y restauración total de los datos para garantizar su uso e integridad.

10.4 Etapa de utilización de los datos

10.4.1 Directrices de seguridad para dispositivos y sistemas

Se recomienda que el software del dispositivo y del sistema esté actualizado y no tenga vulnerabilidades públicas.

Se recomienda que el dispositivo y el sistema tengan instalado software de seguridad actualizado.

10.4.2 Directrices de seguridad para la configuración y gestión

1) Gestión del personal

Se recomienda adoptar una autenticación unificada para diferentes aplicaciones (utilización de datos) a los efectos de acceder a plataformas de macrodatos, con independencia del tipo de interfaces que utilicen las aplicaciones, ya sea la interfaz de programación de aplicaciones de transferencia de estado de representación de recursos (REST API) o la conectividad a bases de datos de Java (JDBC). El mecanismo de autenticación detallado puede ser Kerberos, el protocolo ligero de acceso a directorios (LDAP) u otros.

Se recomienda proporcionar autorización detallada para diferentes aplicaciones a los efectos de acceder a plataformas de macrodatos, en particular los siguientes métodos:

a) Autorización específica para acceder a plataformas de macrodatos mediante nombres de usuario, direcciones del protocolo de Internet (IP) y nombres de aplicaciones (APP);

b) autorización específica para acceder a recursos de almacenamiento, como el software de almacenamiento de datos Hive, la base de datos distribuida, no relacional y de código abierto Hbase, HDFS y diversas DB;

c) autorización específica mediante diferentes operaciones de la DB o el sistema de archivos (por ejemplo, SELECCIONAR, INSERTAR y CREAR);

d) autorización específica de permisos de importación y exportación de datos;

e) autorización específica para el acceso a ficheros y directorio de HDFS.

2) Gestión del dispositivo

Se recomienda proporcionar mecanismos de vigilancia de las actividades maliciosas y aplicación de la normativa en la etapa de utilización de los datos.

Se recomienda dejar rastros de auditoría de seguridad para comprobar la adecuada utilización de los datos, garantizar el cumplimiento de la política de seguridad y los procedimientos operativos establecidos, ayudar a evaluar los daños y recomendar cualquier cambio en los controles de seguridad, la política de seguridad y los procedimientos de utilización de datos.

Se recomienda considerar la posibilidad de aplicar una política de auditoría de seguridad, en cuyo marco se determinen la información sobre la utilización de los datos que debe registrarse, las condiciones en las que debe registrarse esa información y la especificación sintáctica y semántica que debe utilizarse para el intercambio de la información de la auditoría de seguridad.

3) Gestión de datos

A fin de proteger los datos sensibles, es necesario pseudoanonimizar los datos en la etapa de utilización. En la etapa subsiguiente de compartición de datos, se unificarán y considerarán las directrices detalladas para la pseudonimización de datos.

Se recomienda auditar la utilización de datos sensibles, mediante la generación de registros de auditoría, según se indica en [UIT-T X.1641].

10.5 Etapa de compartición de datos

10.5.1 Directrices de seguridad para dispositivos y sistemas

Se recomienda que el software del dispositivo de usuario y del sistema esté actualizado y no tenga vulnerabilidades públicas.

Se recomienda que el dispositivo y el sistema tengan instalado software de seguridad actualizado.

10.5.2 Directrices de seguridad para la configuración y gestión

1) Gestión del personal

Se debe informar a los usuarios sobre qué datos, incluidos los metadatos y cualquier dato resultante de los procesos realizados durante la etapa de utilización, se compartirán con terceros y quiénes son esos terceros. Se debe obtener el consentimiento explícito del usuario antes de compartir cualquier dato, incluidos los datos resultantes.

2) Gestión del dispositivo

Se recomienda controlar la exportación de datos.

Cuando los datos se comparten con servicios externos, se recomienda limitar su utilización a fin de evitar su reventa.

Se recomienda que los mecanismos de protección de la seguridad que se negocien entre las partes interesadas pertinentes (por ejemplo, los operadores entre los que se transfieren los datos), e incluyan una política de seguridad para la transferencia de datos compartidos, el almacenamiento, el acceso, la destrucción y el plan de copias de seguridad si se divulgan datos compartidos.

3) Gestión de datos

La pseudoanonimización de datos es el proceso de ocultar la PII original y los datos sensibles con caracteres o datos. La finalidad es proteger la información personal y los datos sensibles.

Se pueden configurar diferentes aplicaciones con diferentes algoritmos de pseudoanonimización. Se recomienda la pseudoanonimización de datos para:

a) facilitar la adición y eliminación dinámicas de algoritmos de pseudoanonimización;

b) facilitar la pseudoanonimización específica, lo que significa que un administrador puede configurar la pseudoanonimización mediante una tabla o una serie de columnas determinadas en una DB;

c) utilizar algoritmos públicos, evitando los algoritmos patentados de terceros;

d) no afectar de forma significativa a la continuidad de las actividades ni al rendimiento del sistema.

10.6 Etapa de destrucción de datos

10.6.1 Directrices de seguridad para la gestión de datos

Los datos se deben borrar y sobrescribir en estado sólido.

Una vez borrados, se recomienda que el espacio de almacenamiento de recursos, por ejemplo, archivos, directorios y registros de DB, en el sistema quede completamente despejado, sin posibilidad de restauración.

Bibliografía

[b-ITU-T X.800] Recomendación ITU-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

[b-ITU-T X.1040] Recomendación ITU-T X.1040 (2017), *Arquitectura de seguridad de referencia para la gestión de la vida útil de los datos corporativos del comercio electrónico.*

[b-ITU-T Y.3600] Recomendación ITU-T Y.3600 (2015), *Grandes volúmenes de datos – Requisitos y capacidades basados en la computación en la nube.*

[b-ISO/IEC 20889] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques.*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021