Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1750

(09/2020)

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

Seguridad de datos – Seguridad de los macrodatos

Directrices sobre la seguridad de los macrodatos como servicio destinadas a los proveedores de servicios de macrodatos

Recomendación UIT-T X.1750

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.1750

Directrices sobre la seguridad de los macrodatos como servicio destinadas a los proveedores de servicios de macrodatos

Resumen

Los macrodatos como servicio (BDaaS) es una categoría de servicio en la nube que consiste en proporcionar a los clientes de servicios en la nube capacidades para recopilar, almacenar, analizar, visualizar y gestionar macrodatos, como se especifica en la Recomendación UIT-T Y.3600. Con el notable crecimiento de los volúmenes de datos y el rápido desarrollo de empresas de macrodatos, la infraestructura de macrodatos se ha convertido en la principal herramienta para proporcionar BDaaS. En consecuencia, han surgido importantes problemas de seguridad para BDaaS. Por ejemplo, el diseño del software de código abierto para macrodatos no siempre tiene en cuenta la seguridad desde el principio. Las nuevas tecnologías introducidas por el análisis de macrodatos también pueden hacer fracasar las medidas tradicionales de protección de la seguridad. En la Recomendación UIT-T X.1750 se analizan los problemas de seguridad de la BDaaS, se identifican las funciones y responsabilidades de seguridad para prestar el servicio BDaaS y se describe un marco de seguridad para la infraestructura de macrodatos. Asimismo, se especifican las medidas de protección de seguridad que se han de satisfacer para los servicios y componentes relacionados con el BDaaS.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1750	2020-09-03	17	11.1002/1000/14266

Palabras clave

Directrices de seguridad, macrodatos como servicio, medidas de seguridad.

* 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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1750

Directrices sobre la seguridad de los macrodatos como servicio destinadas a los proveedores de servicios de macrodatos

1 Alcance

En la presente Recomendación se analizan los problemas de seguridad de los macrodatos como servicio (BDaaS) y se ofrecen directrices para que los grandes proveedores de servicios de macrodatos (BDSP) protejan los BDaaS. Se identifican las funciones y responsabilidades en materia de seguridad de los componentes de los BDaaS y se especifica un marco de seguridad para una infraestructura de macrodatos, incluyendo plataformas, aplicaciones, análisis, interfaces y el ecosistema de BDaaS. En esta Recomendación también se especifican las medidas de protección de seguridad que deben adoptarse para las actividades o componentes relacionados con los BDaaS.

Esta Recomendación es una descripción de alto nivel de los requisitos de seguridad para la implementación de los BDaaS que se centra en BDaaS. En los BDaaS intervienen los proveedores de infraestructuras de macrodatos (BDIP) y los proveedores de aplicaciones de macrodatos (BDAP). Las directrices para BDAP y BDIP, así como la orientación detallada sobre la implementación de los BDaaS 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.

[UIT-T X.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube.*

[UIT-T X.1631] Recomendación UIT-T X.1631 (2015), *Tecnología de la información – Técnicas de seguridad – Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones.*

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

[UIT-T Y.3600] Recomendación UIT-T Y.3600 (2015), *Big data – Requisitos y capacidades basados en la computación en la nube.*

[ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[ISO 28000] ISO 28000:2007, *Specification for security management systems for the supply chain.*

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los siguientes términos que han sido definidos en otros textos:

3.1.1 macrodatos (*big data*) [UIT-T Y.3600]: Paradigma para hacer posible la recopilación, el almacenamiento, la gestión, el análisis y la visualización, potencialmente en condiciones de tiempo real, de grandes conjuntos de datos con características heterogéneas.

NOTA – Entre los ejemplos de características de los conjuntos de datos figuran el gran volumen, la alta velocidad, la gran variedad, etc.

3.1.2 macrodatos como servicio (*big data as a service* – (BDaaS)) [UIT-T Y.3600]: Una 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, gestionar y visualizar los datos utilizando tecnologías de *big data*.

3.1.3 procedencia de los macrodatos (*big data provenance*) [b-UIT-T Y.3602]: Información que registra la trayectoria histórica de los datos con arreglo a las operaciones del ciclo de vida de los datos en un ecosistema de macrodatos.

3.1.4 computación en la nube [b-UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud.

3.1.5 servicio en la nube [b-UIT-T Y.3500]: Una o varias capacidades que se ofrecen en la computación en la nube que se invoca a través de una interfaz definida.

3.1.6 metadatos [b-UIT-T M.3030]: Datos que describen otros datos.

3.1.7 problema de seguridad [UIT-T X.1601]: "Dificultad" de seguridad diferente a una amenaza de seguridad directa que se debe a la naturaleza y al entorno de funcionamiento de los servicios en la nube, incluidas las amenazas "indirectas".

3.1.8 amenaza [ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.1.9 vulnerabilidad [b-nist sp 800-30]: Punto débil de un sistema de información, de procedimientos de seguridad, de controles internos o de una implementación que podría explotar una fuente de amenaza.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 activos de datos: recurso de datos registrado electrónicamente, poseído o controlado por una organización.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API Interfaz de programación de aplicaciones (*application programming interface*)

ABAC Control de acceso por atributos (*attribute-based access control*)

BDaaS Macrodatos como servicio (*big data as a service*)

BDAP Proveedor de aplicación de macrodatos (*big data application provider*)

BDIP Proveedor de infraestructura de macrodatos (*big data infrastructure provider*)

BDSN Asociados de servicio de macrodatos (*big data service partners*)

BDSP Proveedor de servicios de macrodatos (*big data service provider*)

BDSU Usuario de servicio de macrodatos (*big data service user*)

CSC Cliente de servicio de nube (*cloud service customer*)

DP Proveedor de datos (*data provider*)

PII Información de identificación personal (*personally identifiable information*)

PKI Infraestructura de clave pública (*public key infrastructure*)

SAML Lenguaje de marcaje de aserción de seguridad (*security assertion markup language*)

SDK Paquete de desarrollo de *software* (*software development kit*)

SSL Capa de conexión segura (*secure sockets layer*)

TI Tecnología informática

TLS Seguridad de la capa de transporte (*transport layer security*)

USB Bus en serie universal (*universal serial bus*)

5 Convenios

En la presente Recomendación:

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

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para acreditar la conformidad.

La expresión "**se prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si la Recomendación pretende ser conforme.

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Amenazas y problemas de seguridad para los macrodatos como servicio

En esta cláusula se describen las amenazas y los problemas de seguridad de los macrodatos como servicio (BDaaS). Los servicios BDaaS, basados en la computación en nube, se define en [UIT-T Y.3600]. Para los BDaaS deben tenerse en cuenta los problemas de seguridad correspondientes a los entornos de computación en nube descritos en la cláusula 8 de [UIT-T X.1601]. Así pues, en esta Recomendación se describen las amenazas a la seguridad y los problemas de seguridad relativos a las capacidades y servicios específicos de los BDaaS, es decir, las plataformas de macrodatos como servicio y el software relacionado con los macrodatos como servicio (reconociendo que el ecosistema de BDaaS incluye proveedores de datos (DP), BDAP y BDIP), en particular:

– vulnerabilidades de la infraestructura de macrodatos y fallo de las medidas de seguridad;
– problemas de almacenamiento y auditoría causados por datos no estructurados;
– seguridad y regulación de la interfaz entre aplicaciones, plataformas y flujo de servicio;
– otros problemas de seguridad, por ejemplo, confianza, autentificación y visualización.

En la Figura 6-1 se muestra una arquitectura de los problemas de seguridad de los BDaaS.

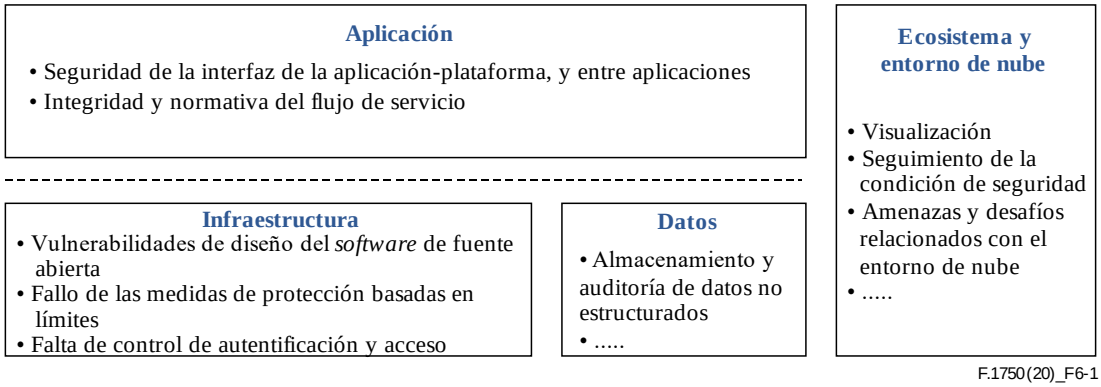

Figura 6-1 – Problemas de seguridad de los macrodatos como servicio

6.1 Problemas de seguridad para una infraestructura de macrodatos

La infraestructura de macrodatos puede consistir en diversos componentes de origen comercial o de código abierto. Es posible que algunos de estos componentes se hayan diseñado sin tener en cuenta la seguridad desde el principio, lo que podría entrañar riesgos de seguridad, entre ellos:

– código fuente inseguro y falta de mecanismos de seguridad en los componentes de código abierto;

– características de plataforma abierta y entre dominios que desdibujan los límites de seguridad tradicionales, causando el fracaso de las medidas de protección basadas en dichos límites; y,

– la falta de mecanismos adecuados de autentificación y control de acceso para las diferentes funciones puede dar lugar a abusos.

6.2 Problemas de seguridad para las aplicaciones de macrodatos

Las infraestructuras de macrodatos integran diversas aplicaciones muy centralizadas con complicados patrones de servicio. Los problemas de seguridad para las aplicaciones de macrodatos incluyen:

– posible carencia de verificación de seguridad y control de transmisión en las interfaces de programación de aplicaciones (API), en los paquetes de desarrollo de software (SDK) y en las interfaces entre aplicaciones; y

– la necesidad de rastrear, auditar y localizar la ejecución de aplicaciones de usuario, a fin de garantizar la seguridad lógica del proceso.

6.3 Problemas de seguridad para los datos

Las infraestructuras y aplicaciones de macrodatos gestionan cantidades masivas de datos. Dentro del ecosistema de macrodatos, los tipos de datos consisten en datos estructurados, semiestructurados y no estructurados. Los datos estructurados suelen almacenarse en bases de datos, organizadas con arreglo a diferentes modelos, por ejemplo, el modelo relacional, el modelo de documentos, el modelo clave-valor, el modelo gráfico, etc. Los datos semiestructurados no se ajustan a la estructura formal de los modelos de datos, pero contienen etiquetas o marcadores para identificar los datos. Y los datos no estructurados no se corresponden con un modelo de datos predefinido y no están organizados de una manera determinada. Los datos pueden estar formatos diferentes, cualquier que sea el tipo de datos, como texto, hoja de cálculo, vídeos, audio, imagen, mapa, etc. (véase [UIT-T Y.3600]). Esos datos se utilizan en las fases de almacenamiento, análisis, cálculo y otras fases del servicio de datos. Los problemas de seguridad de los datos incluyen:

– la exigencia de medidas de seguridad (control de acceso inclusive) para garantizar la confidencialidad de los datos, garantizando a su vez una explotación eficiente de los datos;

– la auditoría de datos no estructurados;

– el riesgo de que se filtre información personal privada, si se trata de datos abiertos o compartidos;
– la necesidad de aplicar a los metadatos las medidas de seguridad tradicionales descritas en [UIT-T X.1601], por cuanto tienen las mismas características que los datos publicados en la web;

Los problemas de seguridad a la hora de gestionar la procedencia de los macrodatos son, entre otros, los siguientes: registros contaminados o manipulados maliciosamente a lo largo de la cadena de procesamiento de la procedencia, participación de entidades no autorizadas en el procesamiento o intercambio de datos de procedencia, códigos de procesamiento no auténticos para la procedencia de los datos, así como problemas de seguridad relativos a los datos de procedencia.

6.4 Problemas de seguridad para el ecosistema de los macrodatos como servicio

Según [UIT-T Y.3600], el ecosistema de BDaaS consiste en funciones y subfunciones desempeñadas por diferentes partes/componentes que proporcionan y consumen servicios de macrodatos. El ecosistema BDaaS es necesario para planificar, diseñar y aplicar medidas de seguridad en la construcción, el funcionamiento, la auditoría y otras fases de la procedencia del servicio. Los problemas de seguridad para los servicios de macrodatos incluyen:

– la necesidad de supervisar continuamente de las acciones de los usuarios, la situación de la red, el estado de los recursos, etc. para hacer frente a las amenazas cambiantes;
– los nuevos vectores de amenazas incipientes y la carencia de posibles mecanismos de protección;
– la incapacidad de instaurar la confianza entre los diversos actores, incluidos los propietarios de los datos y los dispositivos (para recopilar datos);
– la seguridad de la instancia de virtualización, por ejemplo, la configuración de seguridad e integridad de la imagen virtual;
– la posibilidad de que la cadena de suministro sea complicada en el ecosistema de macrodatos, aun cuando un contratista no esté directamente contratado por la organización puede afectar a su continuidad comercial.
– la necesidad de analizar los riesgos relacionados con la cadena de suministro y de adoptar las medidas necesarias, incluidas las medidas de seguridad especificadas en [ISO/CEI 27000] [ISO 28000].

7 Conceptos generales relativos a la seguridad de los macrodatos como servicio y función del BDSP

La Recomendación [UIT-T Y.3600] especifica una arquitectura de tecnología de macrodatos que es general, de múltiples niveles y compuesta por componentes de funciones lógicas. Sobre la base de esta arquitectura, las capacidades de seguridad de los servicios de macrodatos cubren tanto la seguridad del sistema como la seguridad de los datos.

Desde la perspectiva del sistema, los requisitos de seguridad de los BDaaS abarcan las capacidades de cada módulo de función relacionado con 1) la infraestructura de macrodatos; 2) la gestión de aplicaciones de macrodatos; 3) la seguridad de la interfaz; y 4) el funcionamiento y mantenimiento de la seguridad de la plataforma de macrodatos (el ecosistema de los BDaaS).

En particular, [UIT-T Y.3600] describe los BDaaS, que consta de dos componentes principales:

– BDIP: que puede utilizar servicios en la nube de los tipos de capacidad de infraestructura de nube tales como computación como servicio, el almacenamiento de datos como servicio, la infraestructura como servicio y la red como servicio, para prestar servicios de macrodatos con miras a la recopilación de datos, el procesamiento y la gestión de datos.

– BDAP: que ejecuta el análisis de los datos, la visualización y otras aplicaciones de macrodatos.

Desde la perspectiva de los datos, los requisitos de seguridad abarcan cada actividad de datos en el proceso de desarrollo del servicio de macrodatos. Además, las capacidades de seguridad del servicio de macrodatos también incluyen requisitos de seguridad de los metadatos y la cadena de suministro de datos.

Desde el punto de vista del sistema de los BDaaS, [UIT-T Y.3600] identifica el contexto del sistema incluidos las funciones y actividades y los flujos de datos y del servicio.

En cuanto a las funciones [UIT-T Y.3600], los servicios de BDaaS son ofrecidos por el BDSP que se encarga de garantizar la seguridad de los BDaaS y reducir los riesgos. Se recomienda que el BDSP (BDIP y BDAP) considere tanto la seguridad del sistema como la seguridad de los datos para ejecutar las actividades de BDaaS.

8 Medidas de seguridad de los macrodatos como servicio

8.1 Medidas de seguridad para la infraestructura de macrodatos

8.1.1 Seguridad de los activos del sistema

8.1.1.1 Requisitos generales

Los BDSP tendrán que:

– establecer estrategias de gestión de la seguridad de los activos del sistema, y aclarar los objetivos y principios de la seguridad de los activos del sistema;

– establecer políticas y procedimientos de gestión de la construcción y el funcionamiento de los activos del sistema, incluida la planificación, el diseño, la adquisición, el desarrollo, el funcionamiento, el mantenimiento y el desguace;

– establecer un mecanismo de registro de activos del sistema, elaborar una lista de activos del sistema, especificar el problema de la responsabilidad de seguridad y las partes conexas de los activos del sistema, y realizar periódicamente el mantenimiento de la información sobre los activos del sistema;

– establecer y aplicar procedimientos de clasificación y etiquetado de activos del sistema;

– realizar auditorías y actualizaciones periódicas de los activos de la tecnología de la información (TI) y de las políticas de gestión de la seguridad.

8.1.1.2 Requisitos adicionales

Los BDSP deberían:

– identificar los controles de gestión de activos disponibles, como los especificados en [UIT-T X.1631], para realizar el inventario de componentes y el registro, la auditoría y la supervisión de los activos del sistema;

– establecer procedimientos de evaluación del riesgo de los activos para el sistema de macrodatos, por ejemplo, aplicar un proceso para identificar los componentes de productos o servicios que son críticos para mantener la funcionalidad y que, por lo tanto, requieren mayor atención y verificación;

– establecer procedimientos de evaluación de la seguridad de la cadena de suministro, como los definidos en [ISO/CEI 27036-3]. Esto incluye la evaluación de los riesgos de los componentes que ya no están disponibles y los procesos de respuesta a la vulnerabilidad que se repite sistemáticamente.

8.1.2 Seguridad de los activos de datos

8.1.2.1 Requisitos generales

Los BDSP tendrán que:

– establecer estrategias de gestión de la seguridad de los activos de datos, y aclarar los objetivos y principios de la gestión de la seguridad de los activos de datos;

– establecer mecanismos y procedimientos de gestión de la seguridad que abarquen el ciclo de vida de los activos de datos;

– establecer métodos de clasificación y categorización de los activos de datos y guía de funcionamiento en función del valor y la importancia de los activos de datos;

– establecer mecanismos de aprobación de cambios para las estrategias de clasificación y categorización de datos, procedimientos, métodos y guía de funcionamiento;

– establecer especificaciones de seguridad, mecanismos de gestión y procedimientos para la confidencialidad, integridad y disponibilidad de los activos de datos (por ejemplo, estrategia de contraseñas, gestión de claves);

– establecer una lista de activos de datos, identificar el problema responsable de la seguridad de los datos y a las partes pertinentes;

– realizar auditorías y actualizaciones periódicas de las estrategias de gestión de la seguridad de los activos de datos y los procedimientos pertinentes.

8.1.2.2 Requisitos adicionales

Los BDSP deberían:

– establecer principios de gobernanza de la seguridad y políticas de integración de datos para todo tipo de recursos de datos internos y externos;

– establecer la etiqueta correspondiente, el control de acceso a niveles múltiples, el cifrado y descifrado de datos, la desensibilización de datos y otras estrategias de seguridad de acuerdo con la sensibilidad de los activos de datos.

8.1.3 Seguridad del proceso de la cadena de suministro de los datos

8.1.3.1 Requisitos generales

Los BDSP tendrán que:

– aclarar los objetivos, principios y alcance de la gestión de la seguridad de la cadena de suministro de datos;

– elaborar políticas y procedimientos de gestión de la seguridad de la cadena de suministro de datos, incluidos los criterios de gestión de la seguridad de los participantes en la cadena de suministro de datos;

– especificar los propósitos, pautas de suministro y responsabilidades en materia de seguridad de los datos de los participantes en la cadena de suministro de datos mediante acuerdos de cooperación;

– registrar el equipo y las aplicaciones de adquisición y difusión de datos, y registrar y auditar los comportamientos de adquisición y difusión de datos;

– auditar los comportamientos de consumo de datos de los participantes en la cadena de suministro de datos;

– establecer un mecanismo de normalización de la fuente de datos y especificación de la interfaz en la cadena de suministro de datos, registrar y auditar las operaciones importantes;

– establecer la estructura organizativa del funcionamiento y la gestión de la cadena de suministro, el modelo de datos principal de la cadena de suministro, el mecanismo de procesamiento de la calidad de los datos y el mecanismo de rastreo de los datos;
– aclarar las responsabilidades en materia de seguridad de la cadena de suministro de datos, garantizar la autenticidad y la disponibilidad de los servicios de datos conexos;
– garantizar el despliegue de medidas de seguridad en los procesos de suministro de datos, por ejemplo, el intercambio y la utilización de datos;
– establecer catálogos de la cadena de suministro de datos y diccionarios de datos de fuentes de datos, identificar a la parte responsable de la seguridad del proceso de suministro de datos;
– garantizar la fiabilidad del registro a lo largo de la cadena de procesamiento de la procedencia;
– aclarar las entidades responsables de la tramitación de la procedencia de los datos;
– aplicar mecanismos de autentificación para garantizar la autenticidad de las entidades en la cadena de procesamiento e intercambio de los datos de procedencia;
– asegurar la autenticidad de los códigos para la procedencia de los datos y mantener la autenticidad a través de las actualizaciones de los códigos;
– garantizar la confidencialidad, integridad y disponibilidad de los datos de procedencia; dichos requisitos de seguridad se describen en [UIT-T X.1601].

8.1.3.2 Requisitos adicionales

Los BDSP deberían:

– especificar los requisitos de capacidad de servicios de datos para los diferentes participantes en la cadena de suministro de datos, de acuerdo con sus respectivas funciones en el ecosistema de la cadena comercial de datos;
– examinar periódicamente la capacidad de gestión de la seguridad de los datos de los participantes en la cadena de suministro de datos, y evaluar sus riesgos de seguridad;
– evaluar periódicamente el riesgo de seguridad de todo el ciclo de vida de la cadena de suministro de datos.

8.1.4 Seguridad de los metadatos

Se deben tener en cuenta los requisitos de seguridad de datos del cliente de servicio de nube (CSC), tal como se describen en [UIT-T X.1641].

8.1.4.1 Requisitos generales

Los BDSP tendrán que:

– establecer diccionarios de datos y prácticas de gestión pertinentes de acuerdo con la arquitectura empresarial y los servicios de datos, incluidos el dominio de los datos, el tipo de campo, la estructura de las tablas y el modo de almacenamiento lógico y físico;
– establecer metadatos de seguridad y prácticas de gestión pertinentes de acuerdo con la arquitectura de seguridad de los macrodatos, incluida la política de contraseñas, la lista de autoridades y las especificaciones de autorización;
– establecer una estrategia de control de acceso a los metadatos, especificar las funciones de los metadatos y los mecanismos de control de las autorizaciones;
– establecer procedimientos de auditoría de operaciones de metadatos.

8.1.4.2 Requisitos adicionales

Los BDSP deberían:

– crear sistemas de gestión de metadatos para realizar la gestión de unificación de los metadatos de los servicios de macrodatos;

– establecer un mecanismo de categorización automática de los atributos de seguridad de los metadatos de acuerdo con la clasificación y la estrategia de categorización de los bienes;

– establecer una estrategia de etiquetado, incluida la vinculación de los datos y el propietario de los mismos, de acuerdo con los requisitos de seguridad de los metadatos.

8.2 Medidas de seguridad para aplicaciones de macrodatos

8.2.1 Adquisición de recursos de la plataforma

8.2.1.1 Requisitos generales

Los BDSP tendrán que:

– garantizar que los usuarios de servicios de macrodatos estén al tanto y sean notificados de los activos del sistema a los que se accederá mediante una aplicación, como la conexión de red, el servicio de localización y la lista de recursos de equipos como un bus en serie universal (USB) y Bluetooth;

– garantizar que los usuarios de servicios de macrodatos conozcan y sean notificados de los activos de datos sensibles del sistema a los que se accederá mediante una aplicación, como la libreta de direcciones, los registros del sistema y otras fuentes de información sensible;

– garantizar que una aplicación que solicita el acceso a los recursos tenga motivos suficientes para acceder, tal y como se especifica en los documentos proporcionados por el programador de la aplicación.

8.2.1.2 Requisitos mejorados

Los BDSP deberían:

– garantizar que una aplicación limite, en función de las necesidades de la empresa, las comunicaciones de red internas y externas que no sean necesarias o las comunicaciones de red iniciadas por el usuario.

8.2.2 Control de autorización y acceso

8.2.2.1 Requisitos generales

Los BDSP tendrán que:

– establecer la granularidad de la autorización de acceso físico y lógico, la especificación y el mecanismo de control de las aplicaciones de macrodatos, para garantizar que los accesos a los datos relacionados con los servicios de macrodatos y los activos del sistema estén debidamente autorizados;

– establecer medidas de autorización y control de acceso basadas en estrategias de gestión de activos y etiquetas de activos, atributos de seguridad, para garantizar que una aplicación de macrodatos tenga las capacidades de una gestión de control de acceso de grano fino;

– desarrollar una estrategia de control del flujo de información para controlar las operaciones de importación, exportación e intercambio de datos de la infraestructura de macrodatos entre diferentes aplicaciones de macrodatos o la aplicación de macrodatos y el sistema de TI externo;

– implementar la autorización debidamente aprobada de los datos y del acceso a los activos del sistema de personas, grupos, funciones, dispositivos y aplicaciones relacionados con los servicios de macrodatos;

– proporcionar la capacidad de una estrategia de acceso de autorización autodefinida por el usuario sobre la base de los requisitos de servicio, y la autoridad de auditoría otorgada por cada usuario basada en los requisitos de servicio, para asegurar que su acceso se limite al rango mínimo que cumpla con los requisitos del escenario de servicio.

8.2.2.2 Requisitos mejorados

Los BDSP deberían:

– realizar el seguimiento y el control automático de las sesiones de acceso a distancia para detectar los ataques a la red y asegurar la realización de la política de acceso a distancia;

– proporcionar un motor de control de acceso por atributos (ABAC) y funciones de gestión de autorizaciones y control de acceso orientadas al objeto de datos, así como funciones como el punto de administración de las políticas, el punto de decisión de políticas, el punto de imposición de políticas y el punto de acceso de políticas.

8.2.3 Seguimiento del comportamiento de la aplicación

8.2.3.1 Requisitos generales

Los BDSP tendrán que:

– establecer estrategias y procedimientos de seguimiento del comportamiento de la aplicación de macrodatos que abarquen todo el ciclo de vida de los datos;

– dar soporte a los usuarios para personalizar las normas de seguimiento que pueden apoyar el seguimiento y la notificación de operaciones anómalas sobre datos críticos;

– disponer de la capacidad de registrar, realizar el recuento y analizar la información sobre el comportamiento anormal de la aplicación.

8.2.3.2 Requisitos mejorados

Los BDSP deberían:

– establecer mecanismos de gestión del seguimiento del comportamiento de la aplicación orientados a los reguladores y usuarios con requisitos específicos, y proporcionar una interfaz de seguimiento en línea después de la autorización;

– crear una plataforma para registrar y analizar el comportamiento de las aplicaciones de macrodatos, y proporcionar capacidades de análisis de seguridad que permitan identificar el comportamiento de los usuarios e interfaces o componentes de extracción para los protocolos de comunicación de servicios de macrodatos;

– proporcionar sistemas de especificación y directrices de funcionamiento del seguimiento del comportamiento.

8.2.4 Estrategias y procedimiento de seguridad de la aplicación

Los BDSP tendrán que:

– establecer una política de gestión de versiones para las aplicaciones de servicios de macrodatos, aclarar por escrito el procedimiento de autorización y las responsabilidades de las funciones pertinentes – el documento de autorización debe detallar el nombre, la versión, la fuente, el programador, la función, el lugar de despliegue, el resultado de la evaluación de la seguridad y los requisitos específicos de seguridad de las aplicaciones;

– especificar la protección de la transmisión de datos entre las aplicaciones y la infraestructura de macrodatos, así como otros productos de TI auténticos, por ejemplo, aplicar sistemas de seguridad como la capa de conexión segura (SSL) y la seguridad de la capa de transporte (TLS) para cifrar los datos sensibles en la transmisión;

– comprobar las firmas electrónicas de los paquetes de instalación de aplicaciones y los paquetes de actualización;
– garantizar que una aplicación pueda consultar la versión actual del *software* en ejecución, ya sea de forma autónoma o utilizando las funciones pertinentes de la infraestructura de macrodatos;
– garantizar que las aplicaciones puedan tratar operaciones de error predecibles sin afectar el funcionamiento normal de los ecosistemas de macrodatos;
– establecer una política de gestión de actualizaciones y parches para aplicaciones de macrodatos, asegurarse de que las aplicaciones comprueban las actualizaciones e instalan los parches de los componentes;
– seguir las especificaciones de diseño de seguridad de las aplicaciones de macrodatos, evitando las entradas que infringen o eluden las normas de seguridad y las entradas no especificadas;
– concebir mecanismos para evitar la explotación de la vulnerabilidad de las aplicaciones de macrodatos, por ejemplo, evitar la asignación de espacio de memoria con permisos de escritura y ejecución, asignar espacio de memoria con permisos de escritura y ejecución sólo para las funciones de compilación justo a tiempo.

8.2.5 Almacenamiento de credenciales

8.2.5.1 Requisitos generales

Los BDSP tendrán que:

– especificar un método de almacenamiento persistente de credenciales de identidad de la aplicación, incluido el uso de una función de plataforma en lugar de una función de almacenamiento para almacenar todas las credenciales de identidad de forma segura salvo que la propia aplicación realice la función de almacenamiento seguro de credenciales de identidad;
– aclarar la información de credenciales de una aplicación, por ejemplo, la clave, la infraestructura de clave pública (PKI), la clave privada o la contraseña;
– aclarar los métodos de protección de la seguridad y las medidas de control para recopilar, almacenar y utilizar información de identificación personal (PII);
– establecer un proceso de evaluación del método de almacenamiento de credenciales de una aplicación para garantizar que cumple las estrategias de seguridad y los requisitos de procedimiento de los sistemas de servicios de macrodatos.

8.2.5.2 Requisitos mejorados

Los BDSP deberían:

– garantizar que en los documentos de especificaciones de seguridad figuren el propósito y los métodos de almacenamiento persistente de las credenciales de identidad.

8.2.6 Identidad y autentificación

8.2.6.1 Requisitos generales

Los BDSP tendrán que:

– ofrecer la capacidad de gestionar la identidad del usuario, para determinar automáticamente la información sobre la identidad del usuario en aplicaciones de macrodatos para garantizar las relaciones de mapeo entre la identificación del usuario y la información de autorización de la capa de aplicación;
– autentificar la identidad del usuario utilizando más de una técnica de autentificación para el funcionamiento de datos o módulos importantes;

– mostrar información de uso potencialmente útil de los servicios de sistemas de macrodatos a disposición del público, por ejemplo, mostrar la fecha y hora del último acceso o la ubicación del acceso más reciente.

8.2.6.2 Requisitos mejorados

Los BDSP deberían:

– autentificar la identidad del usuario utilizando más de una técnica de autenticación en todas las aplicaciones para un usuario en una posición clave con al menos una técnica basada en un método de certificado biométrico o digital;

– utilizar el lenguaje de marcaje de aserción de seguridad (SAML) de tipo federativo para especificar la identidad y la función, añadir requisitos de seguridad y privacidad, apoyando así las múltiples identidades para acceder a servicios de macrodatos.

8.2.7 Seguridad de configuración por defecto

Los BDSP tendrán que:

– asegurarse, cuando se utilicen credenciales de identidad predeterminadas o cuando no se configure ninguna credencial de identidad, que una aplicación sólo pueda proporcionar funciones esenciales para configurar una nueva identidad, por ejemplo, si se utiliza una contraseña predeterminada para iniciar sesión, un usuario sólo podrá entrar en la interfaz de modificación de la contraseña y la aplicación no deberá proporcionar ninguna otra función hasta que se cambie la contraseña predeterminada;

– proporcionar para las aplicaciones un módulo funcional más seguro y permitir configuraciones de seguridad de un nivel de seguridad más alto en el modo de instalación por defecto, por ejemplo, si una aplicación puede proporcionar un módulo de acceso con contraseña y un módulo de certificado digital al mismo tiempo, en el caso del modo de instalación por defecto, la aplicación elige instalar el módulo de certificado digital;

– limitar los permisos de acceso por defecto para el usuario predeterminado de la aplicación, por ejemplo, impedir que un usuario sin permisos de administrador inicie un programa por defecto;

– garantizar que una aplicación inicie la función de configuración de seguridad de la cuenta de usuario por defecto, incluyendo la longitud de la contraseña, la complejidad de la contraseña, el límite de vida útil y la estrategia de bloqueo de la cuenta;

– garantizar el inicio de las funciones de auditoría de registro necesarias, por ejemplo, la actualización de la instalación de componentes o la modificación de parámetros, cuando se instala una aplicación en la configuración por defecto.

8.2.8 Importación y exportación de datos

8.2.8.1 Requisitos generales

Los BDSP tendrán que:

– formular estrategias y procedimientos de importación y exportación de datos teniendo en cuenta factores como la capacidad de almacenamiento, la velocidad de crecimiento del volumen de datos, las necesidades comerciales, el medio de almacenamiento y el rendimiento, a fin de prevenir importantes pérdidas de datos y reducir los daños causados por su pérdida;

– establecer estrategias y mecanismos de gestión de la exportación de datos, mecanismos de evaluación de la seguridad de las importaciones y exportaciones de datos y un proceso de aprobación de autorizaciones;

– establecer especificaciones de identificación para un medio de almacenamiento de datos exportado – la identificación se ajustará a las normas de denominación unificadas, indicará

los números del medio, el tiempo de exportación, el plazo de validez y otra información importante;

– proporcionar diversos métodos de importación y exportación de datos de multigranularidad, por ejemplo, granularidad de la base de datos, el modelo y el objeto especificado por el usuario;

– realizar la inspección de los resultados de los datos importados y exportados, garantizar la integridad y la validez de los datos;

– registrar los datos de importación y exportación de información operativa, por ejemplo, información sobre la operación, ciclo de operación, número medio, volumen medio, situación de transferencia y almacenamiento, y mantenimiento de registro de cambios pertinentes;

– adoptar mecanismos de cifrado, control de acceso y otras medidas técnicas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos exportados;

– verificar regularmente la integridad y disponibilidad de los datos exportados.

8.2.8.2 Requisitos adicionales

Los BDSP deberían:

– capturar la base de cálculo de los parámetros del índice de la copia de seguridad automática de los datos, incluido el tiempo medio hasta el fallo, el tiempo medio de restauración y el tiempo medio entre fallos, y configurar el correspondiente *software* de importación y exportación automática de datos;

– tener capacidad de importación y exportación de datos a distancia en línea, y realizar periódicamente y de forma semiautomática el almacenamiento a distancia de los datos de usuario;

– almacenar automáticamente la recombinación y compresión de datos de acuerdo con la popularidad de los datos, etc., y asegurar la disponibilidad de datos masivos;

– disponer de una función de almacenamiento de compresión automática para los datos de copia de seguridad del usuario de acuerdo con la frecuencia de la copia de seguridad y restauración de los datos.

8.3 Medidas de seguridad para la interfaz

8.3.1 Requisitos generales

Los BDSP tendrán que:

– proporcionar interfaces de administrador de sistemas, administrador de seguridad, auditor de seguridad y otras interfaces de funciones de usuario y de funciones reguladoras;

– especificar los requisitos de seguridad y las medidas de control de la seguridad para cada interfaz de función, por ejemplo, la autentificación de la identidad, el acceso a la autorización, la firma, el sello de tiempo y el protocolo de seguridad;

– especificar las restricciones de seguridad para el uso de cada clase de interfaz, como las conexiones a distancia cuyas funciones y permisos son limitados;

– aclarar las especificaciones de seguridad de la interfaz de servicio, incluyendo el nombre, los parámetros y los requisitos de seguridad de la interfaz – las especificaciones proporcionan restricciones sobre los parámetros de entrada inseguros y ofrecen la posibilidad de manejar excepciones;

– proporcionar la capacidad de auditar los comportamientos de acceso a la interfaz y las interfaces de servicio de datos configurables;

– adoptar mecanismos de seguridad, como el canal seguro o la transferencia cifrada, para asegurar las interfaces de seguridad entre dominios.

8.3.2 Requisitos mejorados

Los BDSP deberían:

– dar soporte a los requisitos de auditoría en el proceso de acceso a la interfaz y proporcionar las funciones de auditoría y reglamentarias necesarias para el acceso a la interfaz;

– adoptar el método de transmisión de cifrado para la transmisión de la interfaz a través de los dominios de seguridad del sistema;

– llevar a cabo la supervisión y el procesamiento automáticos esenciales del acceso a la interfaz.

8.4 Medidas de seguridad para el ecosistema de macrodatos como servicio

8.4.1 Planificación de la seguridad

La etapa de planificación de la seguridad se divide a su vez en tres subetapas:

– análisis de los requisitos: en la que se identifican, aclaran y definen los requisitos del proceso y de seguridad.

– diseño de la solución: en la que se diseña(n) solución(es) de seguridad.

– evaluación de la solución: en la que se evalúa(n) la(s) solución(es) de seguridad.

Después de esta subetapa, el BDSP puede pasar a la etapa de construcción de la seguridad para su implementación o volver a la subetapa de diseño de la solución para su ajuste o mejora.

8.4.1.1 Análisis de requisitos

8.4.1.1.1 Requisitos generales

Los BDSP tendrán que:

– determinar el alcance de las actividades de proceso de los servicios de macrodatos y los correspondientes requisitos básicos de seguridad para la infraestructura de macrodatos;

– identificar las amenazas específicas a la seguridad, las vulnerabilidades y los riesgos de seguridad a los que se enfrenta una infraestructura de macrodatos y, a continuación, aclarar las medidas técnicas y de gestión de los servicios de macrodatos;

– identificar las prioridades de implementación de los requisitos de seguridad para la infraestructura de macrodatos.

8.4.1.1.2 Requisitos mejorados

Los BDSP deberían:

– establecer el análisis de los requisitos de seguridad y revisar el procedimiento de gestión y garantizar que los requisitos de seguridad para la infraestructura de macrodatos sean íntegros y razonables.

8.4.1.2 Diseño de la solución

8.4.1.2.1 Requisitos generales

Los BDSP tendrán que:

– crear especificaciones técnicas de seguridad de una infraestructura de macrodatos y describir claramente la función de seguridad, la interfaz y los parámetros.

8.4.1.2.2 Requisitos mejorados

Los BDSP deberían:

– demostrar la eficacia de las especificaciones técnicas de seguridad y garantizar que el mecanismo de seguridad no se pueda pasar por alto en el mecanismo de implementación;

– actualizar la solución de seguridad de manera oportuna cuando cambien los requisitos o mejore la tecnología, hasta que se haya completado la evaluación de la solución.

8.4.1.3 Evaluación de la solución

8.4.1.3.1 Requisitos generales

Los BDSP tendrán que:

– revisar periódicamente la propuesta de seguridad para una infraestructura de macrodatos, incluida la arquitectura de seguridad y las líneas básicas de seguridad, asegurándose de que se cumplan los requisitos de seguridad.

8.4.1.3.2 Requisitos mejorados

Los BDSP deberían:

– establecer un sistema de evaluación de la seguridad y determinar un conjunto de factores clave de evaluación.

8.4.2 Construcción de la seguridad

8.4.2.1 Arquitectura de seguridad

8.4.2.1.1 Requisitos generales

Los BDSP tendrán que:

– establecer la arquitectura de seguridad de los servicios de macrodatos y garantizar la validez del proceso de diseño y la realización de los servicios de seguridad de macrodatos descritos en la arquitectura de seguridad;

– garantizar que el dominio de seguridad descrito en los documentos de arquitectura de seguridad sea coherente con las aplicaciones de macrodatos y los requisitos funcionales de la arquitectura de seguridad;

– garantizar que los documentos de arquitectura de seguridad describen el proceso de inicialización de la función de seguridad en las aplicaciones de macrodatos y en la infraestructura de macrodatos, proporcionando así seguridad en la inicialización de la plataforma y las aplicaciones.

8.4.2.1.2 Requisitos adicionales

Los BDSP deberían:

– garantizar que la información contenida en los documentos de descripción de la arquitectura de seguridad sea suficiente para certificar que la función de seguridad de los servicios de macrodatos es capaz de protegerse de la manipulación por parte de sujetos no fiables;

– garantizar que los documentos descriptivos de la arquitectura de seguridad proporcionan un análisis suficiente para demostrar que el mecanismo diseñado para la función de seguridad del servicio de macrodatos no se puede eludir, y que las funciones de seguridad del sistema de macrodatos proporcionadas se han realizado correctamente.

8.4.2.2 Especificación funcional

8.4.2.2.1 Requisitos generales

Los BDSP tendrán que:

– proporcionar especificaciones funcionales que sean precisas y completas, y aclarar la correspondencia entre las especificaciones funcionales y los requisitos de la función de seguridad del servicio de macrodatos;

– garantizar que la especificación funcional facilitada describa íntegramente las funciones de seguridad de los servicios de macrodatos y aclare la relación de la cadena de suministro de datos implicada y los componentes de servicio;
– garantizar que en la especificación funcional facilitada se describa el objetivo de diseño y el método de empleo de todas las interfaces de aplicación de la función de seguridad del servicio de macrodatos y se faciliten todos los parámetros conexos de las interfaces de la función de seguridad.

8.4.2.3 Despliegue de la seguridad

8.4.2.3.1 Requisitos generales

Los BDSP tendrán que:
– establecer un proceso de entrega de seguridad para la entrega de aplicaciones de los programadores a un sistema de servicio de macrodatos;
– describir la función controlada y la autoridad de cada función del servicio de macrodatos en el proceso de despliegue de la seguridad;
– describir las funciones e interfaces disponibles para cada función del servicio de macrodatos, indicar adecuadamente un valor de seguridad, especialmente para todos los parámetros de seguridad controlados por los usuarios;
– describir todas las funciones de los usuarios de los servicios de macrodatos y garantizar que las políticas de seguridad descritas en las especificaciones y políticas de seguridad, necesarias para la seguridad del entorno operativo, se aplican de forma suficiente.

8.4.2.4 Protección de los límites

8.4.2.4.1 Requisitos generales

Los BDSP tendrán que:
– planificar el dominio de la seguridad y el límite de defensa de la seguridad en consonancia con el nivel de seguridad, incluidas las políticas de control de la seguridad y las políticas de gestión;
– planificar el dominio de seguridad y el límite de defensa de la seguridad relacionado con el control del proceso y el aislamiento de las aplicaciones, incluidas las políticas de control de la seguridad y las políticas de gestión;
– desplegar instalaciones de protección de seguridad en el límite del dominio de seguridad, para detectar y protegerse contra incidentes anormales, posibles infracciones, etc.;
– adoptar mecanismos estrictos de defensa de la seguridad comparativa entre los dominios de seguridad, por ejemplo, autentificación de la identidad, gestión de la conexión, política de seguridad del control de acceso a la red, prevención de intrusiones, filtrado de la información y comprobación de la integridad de los límites;
– desarrollar la política de gestión de las instalaciones de defensa de la seguridad y actualizar y adoptar los métodos necesarios para garantizar la implementación de la política.

8.4.2.4.2 Requisitos adicionales

Los BDSP deberían:
– proporcionar medidas y mecanismos personalizados de protección de límites para múltiples arrendatarios;
– especificar un dominio o subdominio de seguridad, un mecanismo de aislamiento de datos entre los dominios de seguridad y un mecanismo de control de acceso para los usuarios o funciones autorizados.

8.4.2.5 Gestión de documentos

8.4.2.5.1 Requisitos generales

Los BDSP tendrán que:

– en un sistema de servicios de macrodatos, implementar la gestión de documentos, cuyo alcance comprenda estrategias, normas y políticas de organización, esquemas del sistema y manuales de aplicación;

– definir los procesos de creación, revisión, aprobación, publicación y archivo de documentos, aclarando las correspondientes responsabilidades de seguridad en cada proceso de gestión de documentos;

– determinar el medio de almacenamiento y los requisitos de tiempo de los documentos, asegurando su disponibilidad e integridad;

– revisar, actualizar, aprobar y publicar periódicamente los documentos, asegurándose de que los usuarios estén al corriente de sus últimas versiones;

– asignar a los organismos responsables el establecimiento y mantenimiento del sistema de gestión de documentos, y ponerlos a cargo del mantenimiento del cambio de versión de los documentos;

– gestionar la clasificación de los documentos del sistema.

8.4.2.5.2 Requisitos adicionales

Los BDSP deberían:

– proporcionar una plataforma para gestionar los documentos en el marco de un proveedor de servicios, asignando diferentes permisos de visualización según las diferentes funciones;

– garantizar la necesaria actualización e identificación de la versión de los documentos correspondientes al actualizar los productos o servicios.

8.4.3 Funcionamiento de la seguridad

8.4.3.1 Gestión de la configuración del sistema

8.4.3.1.1 Requisitos generales

Los BDSP tendrán que:

– formular y ejecutar procedimientos de gestión de la configuración del sistema, establecer la estructura organizativa para la gestión de la configuración del sistema, aclarar las funciones y responsabilidades de los administradores de la configuración, por ejemplo, los administradores de sistemas, los operadores de sistemas, los responsables de seguridad de sistemas, los auditores de sistema, los administradores de bases de datos y otras funciones;

– de conformidad con los requisitos comerciales y los objetos de gestión, estipular los procesos de aprobación, funcionamiento y auditoría de la gestión de la configuración, por ejemplo, los elementos de configuración del anfitrión, los elementos de configuración de la red, los módulos de los servicios de aplicación y otras identificaciones de configuración del sistema, las configuraciones de contenido y las actividades de cambio pertinentes;

– de acuerdo con los resultados de la evaluación, formular una lista de configuración de base de la función de seguridad del sistema de macrodatos y una lista de contenido de comprobación de la configuración diaria, realizando la configuración necesaria para las funciones de seguridad del sistema de macrodatos de acuerdo con el principio del menor privilegio;

– de acuerdo con el acuerdo de nivel de servicio de macrodatos, configurar los parámetros de los productos de TI en el sistema de macrodatos, registrar y mantener la información de configuración de seguridad actual sobre el sistema de macrodatos;

– de conformidad con las estrategias de uso, restringir las estrategias y las políticas de autorización de los programas informáticos adquiridos, prohibir o restringir el uso de determinadas funciones, puertos, protocolos o servicios del sistema de macrodatos;
– aclarar una lista de configuración controlada que requiere cambios regulares, y actualizar periódicamente elementos importantes de configuración del sistema de macrodatos relacionados con la seguridad de la información, por ejemplo, la base de datos de virus, la base de datos de reglas de detección de intrusos, la base de datos de reglas de cortafuegos y la base de datos de vulnerabilidades;
– revisar los cambios presentados a las configuraciones controladas por el sistema de macrodatos, aprobar o rechazar de acuerdo con los resultados del análisis de resultados de seguridad, registrar las decisiones de cambio;
– imponer restricciones a los programadores e integradores de sistemas a la hora de cambiar directamente sistemas de macrodatos, equipos, software y software del fabricante relevantes en el entorno de producción, configuración de auditoría y eventos de cambio;
– antes de proceder a la configuración o introducir un cambio, probar, validar y registrar la configuración controlada y los elementos de cambio, y analizar los elementos de cambio del sistema para estimar su posible impacto en la seguridad de los servicios de macrodatos;
– realizar el seguimiento de los cambios de los parámetros de configuración y habilitar razonablemente las funciones de seguimiento, alerta, defensa y otras funciones del equipo de seguridad;
– proporcionar medidas de respuesta pertinentes para hacer frente a los cambios no autorizados, incluido el personal relacionado con los cambios, la recuperación de la configuración establecida o la interrupción del funcionamiento del sistema informático afectado en situaciones extremas.

8.4.3.1.2 Requisitos adicionales

Los BDSP deberían:

– realizar la gestión de la configuración, efectuar la evaluación de riesgos periódicamente o en el momento en que se produzcan cambios significativos en la arquitectura del proceso o del sistema, revisar los requisitos básicos de configuración y el contenido de la configuración de acuerdo con los resultados de la evaluación, por ejemplo, evaluar riesgos y revisar los requisitos de configuración al menos una vez al año;
– evaluar la estrategia de evaluación de riesgos y sus efectos periódicamente o en el momento en que se produzcan cambios significativos en el proceso o la arquitectura del sistema; según los resultados de la evaluación, revisar los procedimientos de gestión de la configuración del sistema, ajustar la estructura de gestión de la organización, configurar el proceso de gestión, etc.;
– revisar periódicamente las configuraciones de los sistemas de macrodatos, para identificar las funciones, puertos, protocolos o elementos de configuración de servicio innecesarios o inseguros;
– emplear herramientas de configuración de sistemas o mecanismos automáticos para la gestión centralizada, la aplicación y la verificación de los parámetros de los elementos de configuración;
– poder observar en tiempo real los cambios en las infraestructuras de macrodatos y el estado de los recursos virtuales, y disponer de capacidad de ajuste automático para la configuración de la estrategia de seguridad del servicio del sistema.

8.4.3.2 Empleo de servicios de terceros

8.4.3.2.1 Requisitos generales

Los BDSP tendrán que:

– establecer una política de gestión de la seguridad para los socios que prestan servicios como terceros;

– establecer un mecanismo de admisión, evaluación y puntuación para los terceros proveedores de servicios;

– firmar acuerdos de cooperación con terceros proveedores de servicios en materia de componentes de servicios, aclarar sus obligaciones y responsabilidades, por ejemplo, evitar una participación excesiva de terceros proveedores de servicios en el funcionamiento de la seguridad de un sistema de macrodatos;

– garantizar que los componentes de los servicios de terceros incluyan las medidas de seguridad de la información del sistema de macrodatos, apliquen correctamente las medidas de seguridad requeridas y pasen la prueba de los organismos de evaluación de terceros;

– implantar políticas de seguridad del empleo de los componentes con terceros proveedores de servicios, aclarar las condiciones de empleo y el alcance del acceso por parte de los componentes externos;

– adoptar las medidas técnicas o de gestión de la seguridad necesarias para garantizar que los usuarios de macrodatos estén autorizados y habilitados para acceder a los recursos del sistema y de los datos a través de componentes de servicio externos;

– auditar información, como los usuarios, las operaciones previstas y reales de los componentes de servicios externos, y garantizar la trazabilidad de los servicios de macrodatos.

8.4.3.2.2 Requisitos adicionales

Los BDSP deberían:

– evaluar las calificaciones y capacidades de seguridad de los terceros proveedores de servicios y establecer un mecanismo de respuesta de emergencia con los proveedores externos de componentes de servicios basado en la cooperación;

– garantizar que los componentes del servicio externo apliquen correctamente las medidas de seguridad exigidas por la estrategia de seguridad de la información y el plan de seguridad de un sistema de macrodatos, y pasen la prueba de los organismos de evaluación de terceros;

– restringir el uso de recursos de datos sensibles en los componentes de servicios externos por parte de personal autorizado, incluidos los medios de almacenamiento, los archivos de datos y otros recursos de datos controlados por los BDSP.

8.4.3.3 Seguridad de la cadena de suministro de tecnología de la información

8.4.3.3.1 Requisitos generales

Los BDSP tendrán que:

– establecer políticas y procedimientos de seguridad de la cadena de suministro de TI, aclarar el mecanismo de filtrado, el índice de filtrado y el método de evaluación;

– aclarar las funciones y operaciones de los participantes en la cadena de suministro de TI en relación con la adquisición de datos y los servicios de sistemas;

– adoptar las medidas técnicas y de gestión necesarias para la sustitución de la cadena de suministro, y garantizar una respuesta eficaz en caso de que se produzcan incidentes en la cadena de suministro.

8.4.3.3.2 Requisitos adicionales

Los BDSP deberían:

– establecer un modelo de cadena de información de agregación de datos, que incluya la extracción de datos, la integración y la optimización de la fuente de datos de la cadena de suministro;

– establecer un mecanismo de examen y evaluación de la cadena de suministro, realizar una evaluación periódica de los riesgos y una evaluación de la seguridad, por ejemplo, como mínimo una vez al año;

– crear un mecanismo de información relativa a la gestión y evaluación de la calidad de la cadena de suministro de datos.

8.4.3.4 Gestión del sistema de parches

8.4.3.4.1 Requisitos generales

Los BDSP tendrán que:

– establecer procedimientos de gestión de parches, incluidos la descarga, las pruebas, el análisis, la distribución, la instalación, el archivo y otros procesos y contenidos, garantizar la gestión normalizada de los parches del sistema;

– establecer un equipo de gestión de parches, mantenerse al día con la información de divulgación de vulnerabilidades y las respuestas a los eventos de seguridad, realizar la descarga de parches, las pruebas, la instalación y otros trabajos de acuerdo con un calendario apropiado;

– establecer un marco de distribución y gestión de parches del sistema, aclarar los mecanismos de descarga y actualización de parches, por ejemplo, la gestión de parches desencadenada por eventos de seguridad del sistema, o periódicamente con un intervalo fijo;

– disponer de la capacidad de prueba de compatibilidad de los parches antes de la implantación e instalación del parche, y registrar los problemas durante el proceso de actualización del parche;

– poseer la función de comprobación de parches, y verificar que el parche se ha instalado con éxito.

8.4.3.4.2 Requisitos adicionales

Los BDSP deberían:

– establecer un sistema de gestión de parches, actualizar el sistema e instalar parches a través del *software*.

8.4.3.5 Plan de continuidad de las actividades

8.4.3.5.1 Requisitos generales

Los BDSP tendrán que:

– evaluar periódicamente los riesgos que conlleva la actividad continua e informar a los usuarios sobre los riesgos pertinentes;

– formular y aplicar un plan apropiado de copias de seguridad en caso de desastre ajustado a los objetivos estratégicos institucionales, aclarando el nivel, el requisito de recuperación en caso de catástrofe y la estrategia de recuperación de las capacidades de recuperación en caso de colapso del sistema;

– realizar periódicamente el análisis de los efectos sobre el proceso y la evaluación de los riesgos, impartir la capacitación pertinente en materia de continuidad de las actividades.

8.4.3.5.2 Requisitos adicionales

Los BDSP deberían:

– realizar regularmente un experimento de conmutación de sistemas para las infraestructuras pertinentes de los servicios de macrodatos involucrados, optimizar los esquemas de copia de seguridad de los datos y los recursos del sistema de acuerdo con las necesidades reales;

– realizar un simulacro con el plan de continuidad de las actividades para examinar la integridad, operatividad y eficacia del citado plan, verificar la continuidad de las actividades y la disponibilidad de los activos del sistema.

8.4.4 Auditoría de seguridad

Los BDSP deberían llevar a cabo auditorías de seguridad periódicas en todo el ecosistema de BDaaS. La auditoría puede ser ejecutada por un equipo de auditoría interna independiente o por terceros auditores (que actúan como asociados de servicios de macrodatos (BDSN)). Los resultados de la auditoría deben ser debidamente visibles para los BDSU.

8.4.4.1 Gestión de la estrategia de auditoría

8.4.4.1.1 Requisitos generales

Los BDSP tendrán que:

– formular estrategias y procedimientos de auditoría que abarquen el comportamiento de los sistemas de macrodatos y las actividades de los servicios de macrodatos, incluidos el objetivo de la auditoría, el objeto de la auditoría, el funcionamiento de la auditoría, el método de auditoría, la frecuencia de la auditoría, las funciones y responsabilidades pertinentes, el compromiso de la dirección, la coordinación de los participantes en la cadena de suministro y el análisis del cumplimiento;

– formular un proceso de gestión del cambio para las estrategias y procedimientos de auditoría, registrar detalladamente el estado de arranque y parada de las estrategias y procedimientos de auditoría, cambiar la política de rendimiento, la descripción del cambio, etc., revisar y actualizar periódicamente las estrategias y procedimientos de auditoría;

– aclarar los privilegios y responsabilidades de los usuarios en las estrategias y procedimientos de auditoría, establecer el procedimiento pertinente de concesión de privilegios de las estrategias y procedimientos de auditoría, el resultado de las estrategias de auditoría y las funciones de gestión de los datos de auditoría.

8.4.4.1.2 Requisitos adicionales

Los BDSP deberían:

– establecer procedimientos de auditoría de la seguridad de la cadena de suministro de datos y de los mecanismos de coordinación, garantizar la trazabilidad de los eventos de auditoría;

– comprobar y evaluar regularmente la aplicación de las estrategias y procedimientos de auditoría;

– disponer de auditores independientes de la seguridad del sistema, que deben llevar a cabo auditorías de seguridad periódicas en el servicio de macrodatos;

– poseer tecnologías e instrumentos de análisis del cumplimiento para estrategias y procedimientos de auditoría basados en datos de auditoría.

8.4.4.2 Generación de datos de auditoría

8.4.4.2.1 Requisitos generales

Los BDSP tendrán que:

– formular la reglamentación del registro de datos de auditoría, aclarar la estructura y el formato organizativo de los datos de auditoría;

– aclarar los eventos auditables relacionados con las acciones de los sistemas de macrodatos, por ejemplo, inicio de sesión de usuario, gestión de cuentas, acceso de invitados, cambio de estrategia, autorización de funciones privilegiadas, actualización del módulo de servicio;

– aclarar los eventos auditables relacionados con las actividades de datos de los servicios de macrodatos, por ejemplo, la recopilación de datos, el acceso a los datos, el almacenamiento de datos, la transferencia de datos, el procesamiento de datos, el mantenimiento de datos y la destrucción de datos;

– asegurarse de que el registro de datos de la auditoría incluya al menos el tiempo de la operación, el sujeto de la operación, el tipo de operación, el objeto de la operación y los resultados de la operación;

– disponer de capacidades de auditoría de grano fino para las operaciones de datos y las acciones de servicio del sistema;

– mantener una marca de tiempo fiable para el registro de la auditoría; la granularidad del tiempo debe satisfacer los requisitos de la auditoría;

– poseer capacidades de selección y examen de eventos auditables;

– mantener regularmente políticas de registro de datos, eventos auditables y registro de auditoría.

8.4.4.2.2 Requisitos adicionales

Los BDSP deberían:

– proporcionar interfaces de sistema para el acceso a los datos de auditoría de terceros;

– adoptar tecnologías de cifrado para garantizar el no repudio de los datos de auditoría.

8.4.4.3 Protección de los datos de auditoría

8.4.4.3.1 Requisitos generales

Los BDSP tendrán que:

– proporcionar métodos y mecanismos persistentes de gestión de la seguridad del almacenamiento de datos de auditoría masivos;

– poseer capacidades de autorización de acceso a los datos de auditoría, autorizar a las autoridades de acceso a los datos de auditoría a determinados administradores de la auditoría;

– adoptar tecnologías de seguridad o medidas de control para garantizar la autenticidad de los datos de auditoría;

– proporcionar una función de archivo de datos de auditoría, apoyar los métodos y mecanismos de cifrado fuera de línea de los datos de auditoría;

– proporcionar estrategias de gestión y métodos para auditar la eficacia del almacenamiento de datos, la compresión de datos, etc.;

– mejorar la gestión del acceso a los datos de auditoría, registrar todas las operaciones para los datos de auditoría;

– disponer de capacidad de desensibilización para los datos de auditoría exportados;

– garantizar la eficacia del registro de auditoría almacenado si el almacenamiento de la auditoría se agota, se invalida o es objeto de un ataque.

8.4.4.3.2 Requisitos adicionales

Los BDSP deberían:

– disponer de capacidad de recuperación de desastres a distancia y de capacidad para hacer copias de seguridad;

– poder aportar pruebas que demuestren la autenticidad y exhaustividad de los datos de auditoría suministrados.

8.4.4.4 Informe del análisis de auditoría

8.4.4.4.1 Requisitos generales

Los BDSP tendrán que:

– formular estrategias y procedimientos de auditoría, análisis y elaboración de informes para los registros de auditoría;

– examinar y analizar regularmente los registros de auditoría, generar un informe de análisis de auditoría;

– distribuir un informe de análisis al personal responsable especificado de una organización y, si se descubre algún peligro importante para la seguridad o un comportamiento ilegal durante la auditoría, informar a los administradores de la organización lo antes posible.

8.4.4.4.2 Requisitos adicionales

Los BDSP deberían:

– realizar el seguimiento de los eventos auditables y analizarlos en tiempo real, para apoyar el seguimiento y la respuesta frente a acciones sospechosas;

– disponer de capacidades de análisis de correlación de registros de auditoría de diferentes fuentes.

Bibliografía

[b-UIT-T M.3030] Recomendación UIT-T M.3030 (2012), *Marco para un lenguaje de marcaje en telecomunicaciones.*

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Tecnología de la información – Computación en nube – Visión general y vocabulario*.

[b-ITU-T Y.3602] Recomendación UIT-T Y.3602 (2018), *Macrodatos – Requisitos funcionales para la procedencia de los datos*.

[b-NIST SP 800-30] NIST Special Publication NIST SP 800-30 (2012), *Guide for conducting risk assessments*.

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