Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1363

(05/2020)

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

Aplicaciones y servicios con seguridad (2) – Seguridad en la Internet de las cosas (IoT)

Marco técnico para el tratamiento de la información de identificación personal en el contexto de la Internet de las cosas

Recomendación UIT-T X.1363

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.1363

Marco técnico para el tratamiento de la información de identificación personal en el contexto de la Internet de las cosas

Resumen

Los dispositivos de Internet de las cosas (IoT) pueden recabar muchos tipos de datos, incluida la información de identificación personal (IIP). Como los datos IIP son útiles para diferentes tipos de servicios, pueden compartirlos múltiples proveedores de servicios.

En el contexto de la IoT es mejor que cada usuario gestione sus propios datos, incluida la IIP, con arreglo a sus propios fines. Dado que la utilización de datos en el contexto de la IoT con múltiples proveedores de servicios es un asunto complejo, los fines del usuario en cuanto a la utilización de datos deben adaptarse de manera flexible. Por ejemplo, si un proveedor de servicios IoT ofrece las siguientes funciones, el usuario puede considerar que el proveedor de servicios recopila y controla adecuadamente los datos recopilados (incluida la IIP):

– El usuario puede configurar sus preferencias en materia de IIP. Estas preferencias incluyen la lista de datos que es posible compartir con otros proveedores de servicios.
– La recopilación y el intercambio de datos están sujetos a un acceso controlado basado en las preferencias IIP. Los datos no autorizados no se pueden almacenar ni compartir con otros proveedores de servicios.
– El usuario puede verificar el registro histórico de los datos compartidos entre los proveedores de servicios. También puede verificar el instante en que se compartieron sus datos.

En la Recomendación UIT-T X.1363 se especifica un marco técnico para la gestión de la IIP en un entorno de IoT con uno o múltiples proveedores de servicios.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1363	29-05-2020	17	11.1002/1000/140877

Palabras clave

IoT, IIP, información de identificación personal.

* 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.1363

Marco técnico para el tratamiento de la información de identificación personal en el contexto de la Internet de las cosas

1 Alcance

Esta Recomendación especifica un marco técnico para el tratamiento de la información de identificación personal (IIP) en el contexto de la Internet de las cosas (IoT).

En el contexto de la IoT, algunos dispositivos IoT tienen capacidad para recopilar datos IIP. Como éstos son útiles para diversos tipos de servicios, pueden compartirlos múltiples proveedores de servicios. El marco técnico especificado en la presente Recomendación proporciona un mecanismo para proteger los datos IIP del usuario de la IoT cuando se recopilan, comparten y utilizan dichos datos por uno o varios proveedores de servicios IoT.

2 Referencias

Las siguientes Recomendaciones UIT-T y otras referencias contienen disposiciones que, mediante referencia en este texto, constituyen disposiciones de la presente Recomendación. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las Recomendaciones y demás referencias están sujetas a revisión; por lo tanto, se insta a los usuarios de esta Recomendación a que estudien la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias enumeradas a continuación. Se publica periódicamente una lista de las Recomendaciones del UIT-T en vigor. La referencia a un documento en la presente Recomendación no le confiere la categoría de Recomendación.

[UIT-T X.1058] Recomendación UIT-T X.1058 (2017) | ISO/CEI 29151:2017, *Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal*.

[ISO/CEI 29100] ISO/CEI 29100:2011, *Tecnología de la información – Técnicas de seguridad – Marco de privacidad*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 autentificación [b-ISO/CEI 27000]: proporciona garantías de que es correcta la característica alegada de la entidad.

3.1.2 control de acceso [b-ISO/CEI 10027]: capacidad de restringir la utilización de los servicios que acceden a los datos para los usuarios que han sido previamente autorizados.

3.1.3 control [b-ISO/CEI 27000]: medida que modifica el **riesgo** (3.1.16).

NOTA 1 – El control comprende todo **proceso** (3.1.15), **política** (3.1.14), dispositivo, práctica u otras medidas que modifican el **riesgo** (3.1.16).

NOTA 2 – Es posible que el control no siempre produzca el efecto de modificación previsto o supuesto.

3.1.4 dispositivo [b-UIT-T Y.4000]: en el contexto de la Internet de las cosas se trata de una pieza de equipo con las capacidades obligatorias de comunicación y las capacidades opcionales de detección, de accionamiento y de adquisición, almacenamiento y procesamiento de datos.

3.1.5 Internet de las cosas (IoT) [b-UIT-T Y.4000]: infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.

NOTA 1 – Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad.

NOTA 2 – Desde una perspectiva más amplia, IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

3.1.6 sistema de gestión [b-ISO/CEI 27000]: conjunto de elementos interrelacionados o que interactúan de una **organización** (3.1.10) para establecer **políticas** (3.1.14) y **objetivos** (3.1.7) y **procesos** (3.1.15) para lograr dichos objetivos.

NOTA 1 – Los sistemas de gestión pueden ocupar una o varias disciplinas.

NOTA 2 – Los elementos del sistema comprenden la estructura, las funciones y responsabilidad, la planificación y la explotación de la organización.

NOTA 3 – El alcance del sistema de gestión puede abarcar el conjunto de la organización, las funciones específicas e identificadas de la organización, las secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

3.1.7 objetivo [b-ISO/CEI 27000]: resultado que se desea alcanzar.

NOTA 1 – Los objetivos pueden ser estratégicos, tácticos u operativos.

NOTA 2 – Los objetivos pueden guardar relación con diferentes disciplinas (como metas financieras, de salud y seguridad y ambientales) y pueden ser aplicables a diferentes niveles [como estratégico, a nivel de organización, proyecto, producto y **proceso** (3.1.15)].

NOTA 3 – Un objetivo puede expresarse de varias formas, por ejemplo, como un resultado previsto, propósito, un criterio operativo, un objetivo de seguridad de la información o mediante la utilización de otras palabras de significado similar (por ejemplo, propósito, meta o fin).

NOTA 4 – En el contexto de los sistemas de gestión de la seguridad de la información, los objetivos de seguridad de la información los establece la organización, de conformidad con la política de seguridad de la información, con el fin de lograr resultados específicos.

3.1.8 aceptación [b-ISO/TS 17975]: proceso o tipo de política por el que se exige al titular de los datos que tome medidas independientes para expresar su consentimiento previo, específico o explícito para un tipo específico de procesamiento.

3.1.9 denegación [b-ISO/TS 17975]: proceso o tipo de política en virtud del cual se exige al titular de los datos que emprenda una acción independiente para denegar o retirar el consentimiento a un tipo específico de procesamiento.

NOTA – En el caso de denegación, existe el consentimiento implícito para que la organización que recaba los datos procese la información personal a menos que el titular deniegue o retire explícitamente su autorización. La denegación es un proceso que ofrece la organización que recopila datos a fin de que el titular de los datos deniegue o retire su permiso para realizar un tipo de procesamiento específico.

3.1.10 organización [b-ISO/CEI 27000]: persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus **objetivos** (3.1.7).

NOTA – El concepto de organización comprende, entre otros, a un comerciante individual o una compañía, corporación, firma, empresa, autoridad, sociedad, institución organización benéfica o institución, o parte o combinación de ellas, ya sea incorporada o no, pública o privada.

3.1.11 información de identificación personal [ISO/CEI 29100]: toda información que a) puede utilizarse para identificar el titular de la información de identificación personal (IIP) con quien está relacionada esa información; o b) está o puede estar relacionada directa o indirectamente con el titular de la IIP.

NOTA – Para determinar si un titular de IIP es identificable, se deben tener en cuenta todos los medios utilizables, razonablemente, por el interesado en la privacidad que posea los datos, o por cualquier otra parte, para identificar a esa persona física.

3.1.12 preferencias de información de identificación personal [ISO/CEI 29100]: opciones específicas tomadas por el titular de la información de identificación personal (IIP) acerca de cómo se debe procesar su IIP para un fin en concreto.

3.1.13 titular de información de identificación personal [ISO/CEI 29100]: persona física con quien está relacionada la información de identificación personal.

NOTA – En función de la jurisdicción y de la legislación sobre privacidad y protección de datos concreta, también puede utilizarse el sinónimo "sujeto de los datos" en vez del término "titular de la IIP".

3.1.14 política [b-ISO/CEI 27000]: intenciones y orientación de una **organización** (3.1.10), manifestados oficialmente por sus **altos directivos** (3.1.18).

3.1.15 proceso [b-ISO/CEI 27000]: conjunto de actividades interrelacionadas o que interactúan que transforma las entradas en salidas.

3.1.16 riesgo [b-ISO/CEI 27000]: efecto de la incertidumbre en los **objetivos** (3.1.7).

3.1.17 objeto [b-UIT-T Y.4000]: en el contexto de la Internet de las cosas se trata de un elemento del mundo físico (objeto físico) o del mundo de la información (objeto virtual) que se puede identificar e integrar en las redes de comunicaciones.

3.1.18 alta dirección [b-ISO/CEI 27000]: persona o grupo de personas que dirigen y controlan la **organización** (3.1.10) a su más alto nivel.

NOTA 1 – La alta dirección tiene la potestad de delegar autoridad y proporcionar recursos dentro de la organización.

NOTA 2 – Si el alcance del **sistema de gestión** (3.1.6) abarca sólo una parte de una organización, entonces la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización.

NOTA 3 – La alta dirección se denomina a veces dirección ejecutiva y consiste en los directores ejecutivos, directores financieros, directores de información y funciones similares.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Siglas y acrónimos

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

ACT Tabla de control de acceso (*access control table*)

IIP Información de identificación personal

IoT Internet de las cosas (*Internet of things*)

T&C Términos y condiciones

5 Convenios

Ninguno.

6 Consideraciones generales

Existen muchos tipos de dispositivos IoT y algunos de ellos son capaces de recabar datos IIP. Dado que los datos IIP son útiles para diversos tipos de servicios, los proveedores de servicios tienden a recopilar muchos tipos de datos IIP de los usuarios. Además, los datos IIP recopilados por un proveedor de servicios puede compartirlos con otros proveedores de servicios para prestar colectivamente servicios que sean más útiles para los usuarios. En este caso, hay dos tipos de proveedores de servicios, uno que recopila los datos (IIP) de los usuarios y otro que presta diversos servicios utilizando los datos recabados por otros proveedores de servicios.

Desde el punto de vista del usuario, estos proveedores de servicios deben darles un tratamiento adecuado a sus datos IIP. Se recomienda que los usuarios especifiquen cómo desean que se traten sus datos, en particular la IIP, en el contexto de la IoT. Dado que la utilización de datos en el contexto de la IoT con múltiples proveedores de servicios es un asunto complejo, la utilización de los datos prevista por el usuario debe adaptarse de manera flexible. Por ejemplo, si el proveedor de servicios IoT ofrece las siguientes funciones, el usuario puede considerar que el proveedor de servicios recopila datos y trata los datos IIP adecuadamente:

– El usuario puede configurar sus preferencias en materia de IIP. Estas preferencias incluyen la lista de datos que permite compartir con otros proveedores de servicios.

– La recopilación y el intercambio de datos están sujetos a un acceso controlado basado en las preferencias IIP. Los datos no autorizados no se pueden almacenar ni compartir con otros proveedores de servicios.

– El usuario puede verificar el registro histórico de los datos compartidos entre los proveedores de servicios. También puede verificar el momento en que se compartieron sus datos.

7 Modelo de servicio IoT con uno o varios proveedores de servicios

La Figura 1 ilustra el modelo de servicio IoT para los servicios prestados por un proveedor de servicios. En este caso, el proveedor de servicios recaba diferentes tipos de datos (IIP inclusive) y guarda la información en un sistema de almacenamiento de datos administrado por el proveedor de servicios. El proveedor de servicios ofrece diversas aplicaciones a los usuarios que facilitan sus datos (IIP inclusive) al proveedor de servicios.

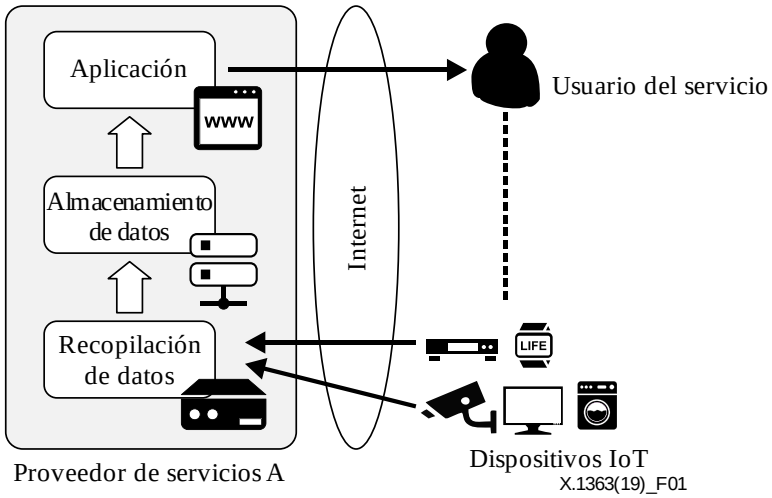

Figura 1 – Modelo para un solo proveedor de servicios

En este modelo de servicio IoT, el único proveedor de servicios trata los datos recopilados y los usuarios utilizan las aplicaciones con arreglo a los términos y condiciones (T&C) aceptados.

La Figura 2 ilustra el modelo para múltiples proveedores de servicios que comparten los datos recabados de los dispositivos IoT. En este caso, hay dos tipos de proveedores de servicios: el "proveedor de servicios de datos" y el "proveedor de servicios de aplicaciones". En la Figura 2, el proveedor de servicios A recopila datos (IIP inclusive) de los dispositivos IoT y los comparte con otros proveedores de servicios (proveedores de servicios B y C). El proveedor de servicios A se denomina "proveedor de servicios de datos" y los proveedores de servicios B y C se denominan "proveedores de servicios de aplicaciones". Un proveedor de servicios puede actuar como "proveedor de servicios de datos" y como "proveedor de servicios de aplicaciones".

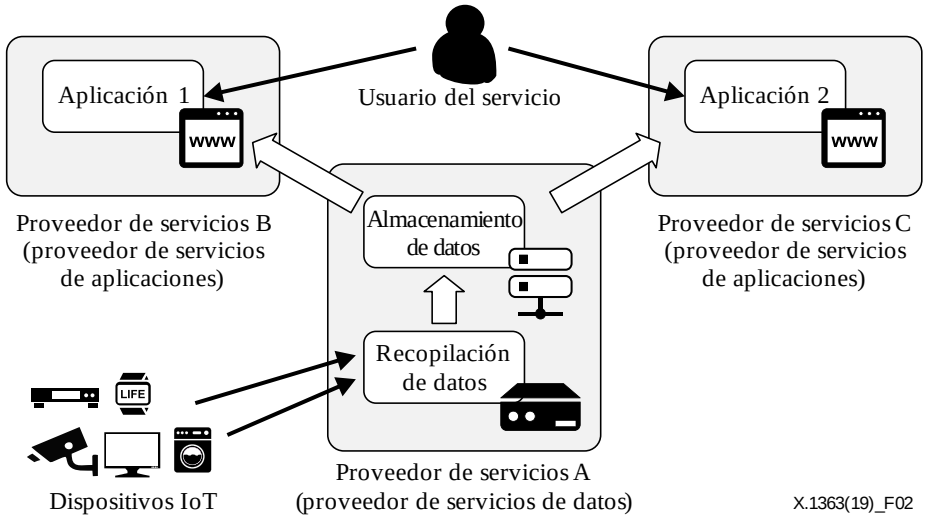

Figura 2 – Modelo para múltiples proveedores de servicios

Por lo general, la lista de datos compartidos con otros proveedores de servicios se incluye en los T&C del proveedor de servicios de datos y los usuarios deben dar su consentimiento antes de poder utilizar los servicios de dicho proveedor.

La principal diferencia entre el modelo para un solo proveedor de servicios único y el modelo para múltiples proveedores de servicios radica en si los datos recabados por los dispositivos IoT se comparten o no con otros proveedores de servicios de aplicaciones. En el caso del modelo para múltiples proveedores de servicios, los datos recopilados por los dispositivos IoT se transfieren a otros proveedores de servicios de aplicaciones.

8 Cuestiones relativas al tratamiento de datos IIP por los servicios IoT

Los proveedores de servicios IoT deben considerar las siguientes cuestiones al tratar los datos IIP:

– Finalidad de la recopilación de datos IIP

Para evitar la recopilación innecesaria de datos desde el punto de vista de un usuario, los usuarios deben conocer con qué fin se recaban datos y la naturaleza de los datos recogidos para el servicio IoT.

– Consentimiento obligatorio para la recopilación de datos IIP

Cuando el usuario se suscribe a un servicio IoT, el proveedor de servicios de datos debe obtener su consentimiento para recopilar diversos tipos de datos IIP. Por lo general, esta información figura en los T&C del proveedor del servicio de datos y el usuario debe dar su consentimiento antes de poder suscribirse al servicio.

– Transferencia de datos IIP a terceros

Los datos recabados de los dispositivos IoT pueden compartirse con terceros, es decir, con otros proveedores de servicios. En este caso, el proveedor de servicios de datos debe obtener el consentimiento explícito del usuario antes de poder transferir sus datos IIP a terceros, antes de poder enviarlos a otros proveedores de servicios. En la mayoría de los casos, el usuario no puede controlar la transferencia de datos IIP. Por ejemplo, el usuario no puede seleccionar a quién se transfiere sus datos IIP, ni configurar qué tipo de datos IIP pueden compartirse. Además, el usuario no puede saber qué tipo de datos personales se envían a terceros.

– Aceptación y denegación del consentimiento para recopilar/transferir datos IIP

Cuando un servicio emplea datos IIP del usuario, el proveedor de servicios de datos debe obtener el consentimiento del usuario tanto para recopilar datos personales del usuario como para transferirlos a terceros. No sólo es importante el momento en que se recibe el consentimiento, sino también el método para obtenerlo (aceptación o denegación).

9 Principios relativos al tratamiento de datos IIP por los servicios IoT

Los principios y controles de la protección IIP se especifican en [ISO/CEI 29100] e [UIT-T X.1058], y se establecieron a partir de diversos principios de protección de la IIP vigentes en varios países, Estados y organizaciones internacionales, como la Organización para la Cooperación y el Desarrollo Económico (OCDE) y la Cooperación Económica de Asia-Pacífico (APEC).

En las cláusulas 9.1 y 9.2 se describen los principios para el tratamiento de datos IIP por los servicios IoT para satisfacer estos principios en [ISO/CEI 29100] y [UIT-T X.1058].

9.1 Principios generales relativos al tratamiento de datos IIP por los servicios IoT

La IIP puede utilizarse para identificar, contactar o localizar a una determinada persona. La divulgación de dicha información puede dar lugar al robo de identidad u otros usos fraudulentos, causando así daños importantes, bochornos e inconvenientes para las personas [b-GAO-08-343]. Por lo tanto, el tratamiento de los datos IIP por los servicios IoT debe cumplir los siguientes principios generales:

1) Cifrado de datos IIP

Se cifrarán todas las IIP almacenadas en dispositivos IoT o en las bases de datos. Además, todas las IIP se cifrarán durante la transmisión dentro de todos los componentes de servicio IoT y entre ellos (es decir, dispositivo IoT, almacenamiento de datos y aplicación).

2) Control de acceso/autentificación

Si los datos IIP se almacenan en dispositivos IoT o en bases de datos del servicio (almacenamiento de datos), se aplicarán los controles de acceso adecuados. La autorización para acceder a la IIP se limitará exclusivamente a la utilización prevista para la que el proveedor de servicios haya solicitado el consentimiento. Esta utilización prevista se incluirá en los T&C cuyo consentimiento haya obtenido del usuario el proveedor del servicio. También se restringirá el acceso cuando exista la posibilidad de que exista una posible vinculación entre los conjuntos de datos almacenados que pudiera dar lugar a la identificación o inferencia no autorizada de PII.

3) Registro

La creación de extractos de datos legibles por ordenador que consten de IIP se mantendrá en un registro oficial que incluya el creador, la fecha, el tipo de información, la finalidad de la extracción y el usuario. Toda IIP que se incluya en estos registros (por ejemplo, nombre de usuario) se cifrará y estará sujeta a controles de acceso.

4) Cifrado para comunicación

Los datos IIP se cifrarán u ocultarán si se comparten entre múltiples proveedores de servicios.

5) Notificación en caso de datos comprometidos

Si los datos IIP se ven comprometidos debido a la violación, filtración, uso o manipulación indebidos de los datos en cualquier punto del servicio IoT, el proveedor de servicios notificará a los usuarios afectados y a los proveedores de servicios pertinentes inmediatamente después de que se descubra la existencia de dicha filtración.

6) Procedimientos para la retención mínima de datos

El almacenamiento de datos IIP, ya sean recopilados u obtenidos como resultado del tratamiento de datos realizado por un proveedor de servicios, se limitará exclusivamente al objeto específico para el que el proveedor de servicios haya obtenido el consentimiento explícito. El proveedor de servicios establecerá un periodo máximo de conservación de los datos IIP en función de la utilización prevista de los mismos, de la posibilidad de que se establezca un vínculo entre los conjuntos de datos almacenados que pudiera dar lugar a la identificación o inferencia de PII adicionales y de las disposiciones legales y reglamentarias nacionales aplicables.

9.2 Principios de la tratamiento de datos IIP

Los proveedores de servicios de datos que recopilan datos IIP a partir de los dispositivos IoT también deben tratarlos adecuadamente. En particular, si los datos son utilizados por los servicios y compartidos con otros proveedores de servicios, su tratamiento debe satisfacer la utilización prevista del usuario. Por consiguiente, el tratamiento de los datos IIP por parte de los proveedores de servicios IoT debe cumplir los siguientes principios:

1) Explicación de la finalidad de la recopilación de datos IIP

A fin de recopilar los datos IIP mínimos necesarios de los usuarios para prestar un servicio IoT, el proveedor de servicios explicará en los T&C con qué finalidad se recopilan los datos y el periodo durante el que se conservarán los datos IIP recopilados.

2) Consentimiento explícito para recopilar y compartir datos IIP del usuario

Cuando un proveedor de servicios suministre servicios que recopilan datos IIP de los usuarios, deberá obtener el consentimiento explícito del usuario para la recopilación y el intercambio de datos. En particular, el proveedor de servicios aplicará un modelo de aceptación previa siempre que sea posible para obtenerlo.

3) Transparencia en la utilización de datos IIP

Cuando los datos IIP, incluida cualquier IIP obtenida mediante el tratamiento de datos realizados por el proveedor de servicios, se compartan con otros proveedores de servicios, el proveedor de servicios garantizará la transparencia del mecanismo de gestión de IIP para que los usuarios puedan verificar cómo se utilizan sus datos IIP. El servicio IoT también ofrecerá un mecanismo de reparación al que podrán recurrir los usuarios en caso de que se atribuyan indebidamente sus datos.

4) Control de las preferencias propias

Los datos IIP se tratarán con arreglo a las preferencias en materia de IIP configuradas por el usuario.

10 Tratamiento de datos IIP en el contexto de la IoT

10.1 Marco básico para el tratamiento de datos IIP en un entorno de IoT

La Figura 3 ilustra el maco básico para el tratamiento de datos IIP en el contexto de la IoT.

Al principio, los usuarios deciden sus preferencias sobre el tratamiento de datos IIP y lo recogen en sus preferencias en materia de IIP en el gestor de preferencias IIP. Los datos (IIP inclusive) proporcionados por los usuarios se controlan en función de las preferencias IIP.

Las preferencias en materia de IIP pueden incluir los siguientes elementos:

– Tipos de datos recabados por los dispositivos IoT – Los dispositivos IoT deben recabar solamente los datos IIP para los que el usuario haya dado su consentimiento explícito en sus preferencias IIP.

– Momento en que se recopilan los datos por los dispositivos IoT (por ejemplo, día laborable entre las 09.00 y las 17.30 horas) – Los usuarios no desean que sus datos IIP se envíen en cualquier momento, por lo que dicho instante debe configurarse en las preferencias IIP.

– Proveedores de servicios autorizados con los que se pueden compartir datos IIP – El usuario puede seleccionar a los proveedores de servicios de aplicaciones que podrán acceder a sus datos IIP. Los usuarios también pueden elegir los tipos de datos IIP a los que pueden acceder los proveedores de servicios de aplicaciones, comprendidos los datos recopilados mediante los dispositivos IoT o generados mediante el tratamiento de datos realizado por el proveedor de servicios primario.

Antes de comenzar a recopilar y utilizar datos, los componentes de servicio IoT, tales como los dispositivos IoT, el almacenamiento de datos, las aplicaciones, etc., deben comprobar las preferencias IIP y tratar los datos en consecuencia.

En segundo lugar, se genera la información de control de acceso a partir de las preferencias IIP y se actualiza la tabla de control de acceso (ACT) utilizando esta información.

En tercer lugar, cada componente consulta esta ACT en caso de que recopile o transfiera datos IIP. La información de control de acceso de la ACT se utiliza para controlar qué tipo de datos IIP puede transferirse entre los componentes de servicio IoT.

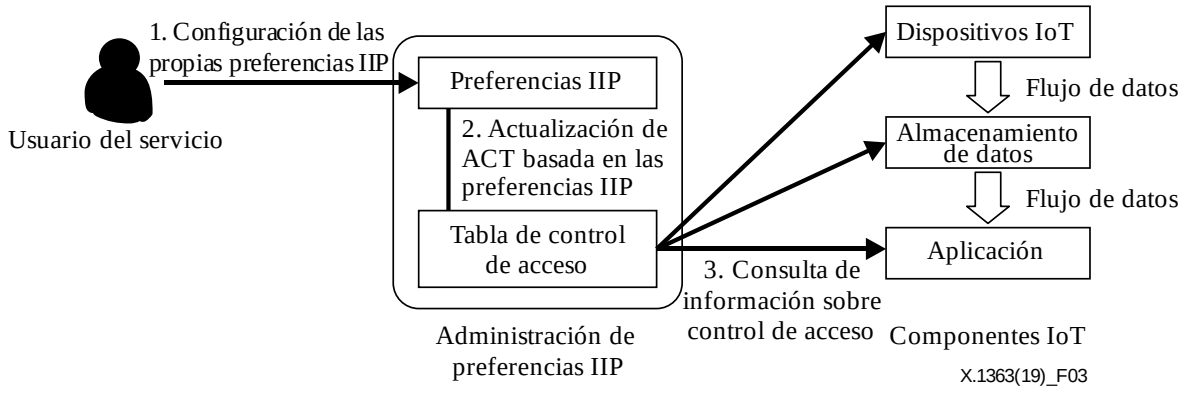

Figura 3 – Marco básico para el tratamiento de datos IIP

10.2 Principios relativos a la interfaz de usuario para configurar las preferencias IIP

A fin de implementar este marco básico, los proveedores de servicios deben proporcionar una interfaz de usuario para que los usuarios puedan configurar sus preferencias IIP. Esta interfaz de usuario debe cumplir los siguientes principios:

1) Fácil acceso para todos los usuarios

Todos los usuarios podrán acceder fácilmente a la interfaz de usuario. Por ejemplo, la primera pantalla de los servicios ofrecidos debe tener un enlace a dicha interfaz de usuario.

2) Control de acceso adecuado a la interfaz de usuario

Cada usuario de servicio tiene sus propias preferencias en materia de IIP. Por lo tanto, cada usuario tendrá una cuenta de usuario única y se autentificará de forma segura, por ejemplo, utilizando la autenticación de dos factores, antes de permitirle acceder a su cuenta de usuario.

3) Exhaustivo

La interfaz de usuario gestionará todas las preferencias IIP, comprendida la recopilación y el intercambio de datos IIP, de un usuario en un mismo lugar.

4) Fácil de utilizar

La interfaz de usuario deberá ser fácil y sencilla para que el usuario pueda configurar sus preferencias en materia de IIP.

11 Marco técnico para el tratamiento de datos IIP en el contexto de la IoT

En esta cláusula se explica cómo aplicar el marco básico especificado en la cláusula 10 para el tratamiento de los datos IIP en el contexto tanto de uno como de varios proveedores de servicio.

11.1 Tratamiento de datos IIP de los servicios IoT por un solo proveedor de servicios

11.1.1 Modelo de referencia para los servicios IoT prestados por un solo proveedor de servicios

La Figura 4 ilustra el modelo de referencia para los servicios IoT prestados por un solo proveedor de servicios. En este caso, el proveedor de servicios proporciona todas las funciones correspondientes a los servicios IoT. El proveedor de servicios recaba datos (IIP inclusive) de los dispositivos IoT y los guarda en el almacenamiento. Además, puede prestar servicios de aplicaciones a los usuarios mediante los datos recabados.

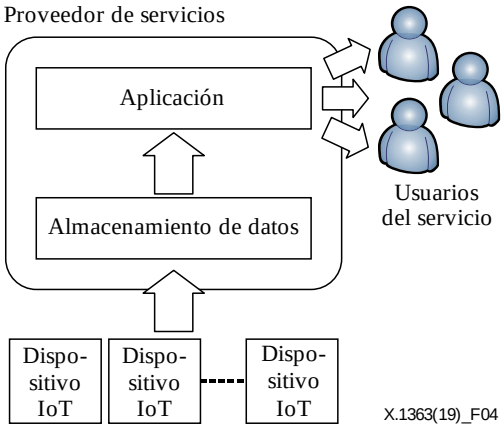

Figura 4 – Modelo de referencia para servicios IoT prestados por un solo proveedor de servicio

11.1.2 Marco técnico para el tratamiento de datos IIP por un solo proveedor de servicios

La Figura 5 ilustra el marco técnico para el proveedor de servicios que dispone de un administrador de preferencias IIP que se encarga de gestionar las preferencias IIP de los usuarios. Los usuarios configuran sus preferencias IIP a través de este administrador de preferencias IIP y los componentes de servicio IoT, como el dispositivo IoT, el almacenamiento de datos y la aplicación, tratan los datos IIP basándose en esa configuración. Por ejemplo, si el usuario desea limitar los datos IIP específicos recopilados por los dispositivos IoT, los dispositivos IoT no deben, en consecuencia, enviar dichos datos IoT al almacenamiento de datos.

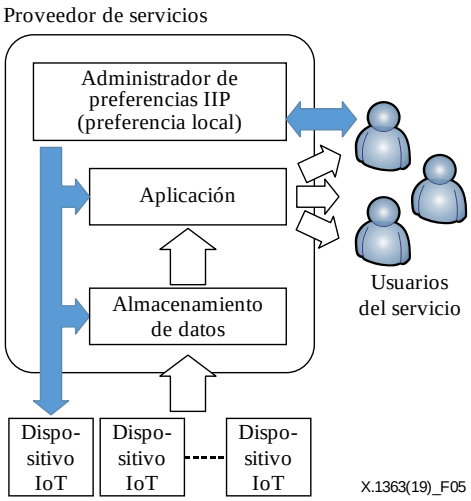

Figura 5 – Marco técnico para el tratamiento de datos IIP por un solo proveedor de servicios

11.1.3 Marco técnico para el tratamiento de datos IIP por un solo proveedor de servicios con un portal común para la administración de preferencias IIP

Cuando los servicios IoT los presta un solo proveedor, los datos recopilados por los dispositivos IoT no se comparten con otros proveedores de servicios a cuyos servicios IoT no recurre ese usuario. No obstante, podría ser necesario que los proveedores de servicios compartieran cierta información básica común sobre las preferencias IIP, por cuanto configurar por los usuarios sus preferencias IIP para cada uno de los servicios IoT llevaría demasiado tiempo. Si el usuario puede especificar preferencias IIP comunes para cualquier tipo de servicio IoT, resultará más fácil y eficaz la configuración de preferencias IIP para cada servicio individual. Para ello, hay dos tipos de administradores de preferencias IIP.

La Figura 6 ilustra un marco técnico para dos componentes del administrador de preferencias IIP, uno de los cuales sigue siendo el administrador de preferencias IIP que pertenece al proveedor de servicios, y el otro es un portal de administración de preferencias IIP que se utiliza para administrar las preferencias comunes a cualquier servicio IoT y para el acceso por otros proveedores de servicios.

En este caso, las preferencias comunes del usuario para cualquier servicio se almacenan en el portal de administración de preferencias IIP, mientras que sus preferencias específicas para cada servicio concreto se almacenan en el administrador de preferencias IIP administrado por cada proveedor de servicios. Cuando el usuario se inscribe a un nuevo servicio, el administrador de preferencias IIP local del proveedor de servicios de datos consulta sus preferencias comunes del portal de administración de preferencias IIP, que puede ser administrado por un tercero y configurado de antemano por el usuario. Aunque el usuario todavía necesita configurar sus preferencias IIP con el administrador de preferencias IIP local para ese servicio específico, no necesita configurar cada vez sus preferencias comunes, que están almacenadas en el portal de administración de preferencias IIP. Los componentes de servicio IoT, tales como los dispositivos IoT, almacenamiento de datos y aplicación, controlan los datos IIP basados en las preferencias locales contenidos en el administrador de preferencias IIP.

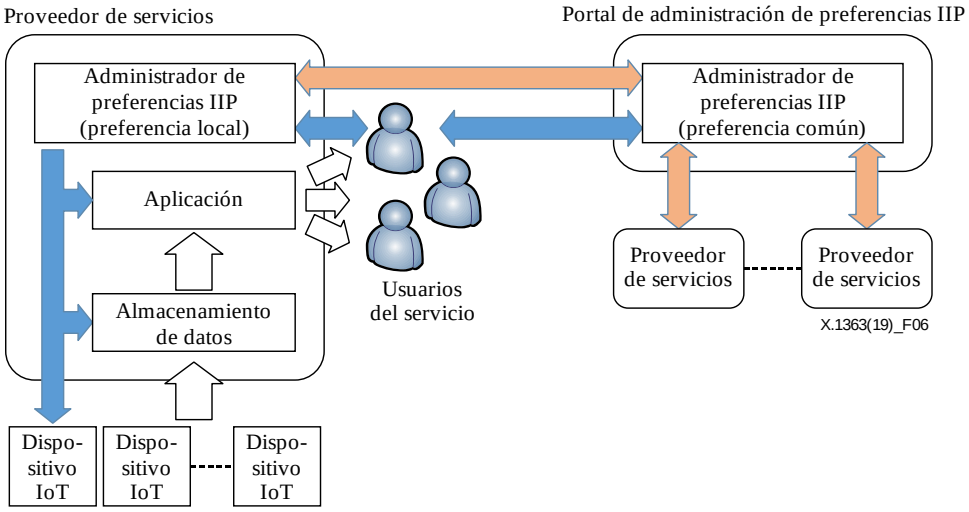

Figura 6 – Marco técnico para el tratamiento de datos IIP por un solo proveedor de servicios con un portal común para la administración de preferencias IIP

11.2 Tratamiento de datos IIP del servicio IoT por múltiples proveedores de servicios

11.2.1 Modelo de referencia para servicios IoT por múltiples proveedores de servicios

La Figura 7 ilustra un modelo de referencia para los servicios IoT prestados por múltiples proveedores de servicios. En este caso, el servicio IoT consiste en múltiples proveedores de servicios (proveedor de servicios de aplicaciones y proveedor de servicios de datos), y cada proveedor de servicios de aplicaciones proporciona sus propios servicios a los usuarios utilizando datos recopilados por otro proveedor de servicios de datos. Por consiguiente, los proveedores de servicios que recopilan datos (IIP inclusive) de los dispositivos IoT (proveedor de servicios de datos) pueden ser diferentes de los que sólo prestan servicios a los usuarios (proveedor de servicios de aplicaciones). En la Figura 7 hay dos tipos de proveedores de servicios: uno es un "proveedor de servicios de datos" que recopila los datos (IIP inclusive) de los dispositivos IoT y los otros son "proveedores de servicios de aplicaciones" que prestan servicios de aplicaciones a los usuarios que utilizan los datos recopilados.

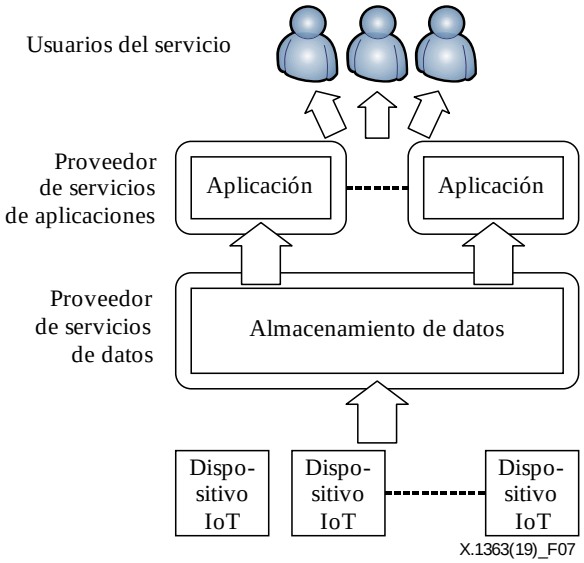

Figura 7 – Modelo de referencia para servicios IoT prestados por múltiples proveedores de servicios

11.2.2 Marco técnico para el tratamiento de datos IIP por múltiples proveedores de servicios

La Figura 8 ilustra un marco técnico para el proveedor de servicios de datos con un administrador de preferencias IIP y en el que todas las preferencias de los usuarios acerca del tratamiento datos IIP se administran en este componente de administración local. Los usuarios configuran sus preferencias locales con el administrador de preferencias IIP. Los componentes del servicio IoT (incluidas las aplicaciones suministradas por otros proveedores de servicios de aplicaciones) tratan los datos IIP basándose en las preferencias locales del administrador de preferencias IIP del proveedor de servicios de datos.

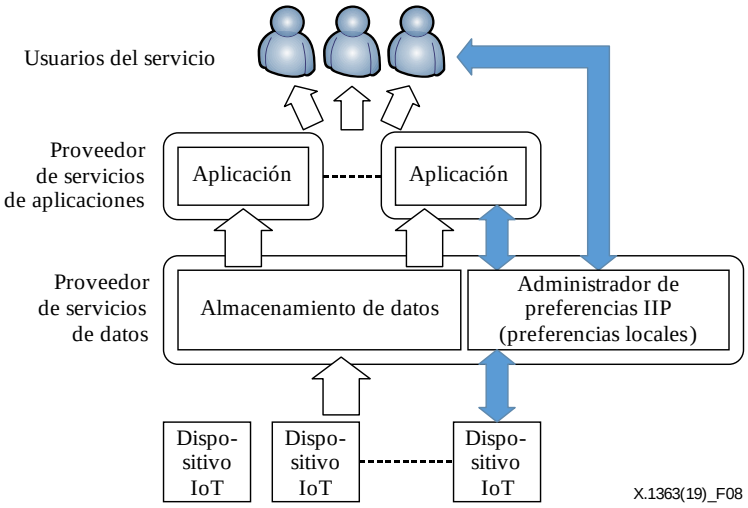

Figura 8 – Marco técnico para el tratamiento de datos IIP de servicios IoT prestados por múltiples proveedores de servicios

11.2.3 Marco técnico para el tratamiento de datos IIP por múltiples proveedores de servicios con un portal común para la administración de preferencias IIP

La Figura 9 ilustra el marco técnico para múltiples proveedores de servicios que utilizan tanto las preferencias IIP almacenadas en un portal común de administración de preferencias IIP como en los administradores locales de preferencias IIP de los proveedores de servicios de datos.

En este caso, las preferencias comunes para cualquier servicio se almacenan en un portal común de administración de preferencias IIP, mientras que las preferencias específicas de cada servicio se almacenan en un administrador de preferencias IIP local administrado por cada proveedor de servicios de datos. Cuando el usuario se inscribe a un nuevo servicio, el administrador de preferencias IIP local del proveedor de servicios consulta las preferencias comunes del portal de administración de preferencias IIP. Aunque este usuario todavía necesita configurar sus preferencias IIP en el administración de preferencias IIP local, no necesita configurar de nuevo las preferencias IIP comunes almacenadas en el portal de administración de preferencias IIP. Los componentes del servicio IoT controlan los datos IIP basándose en las preferencias locales del administrador de preferencias IIP.

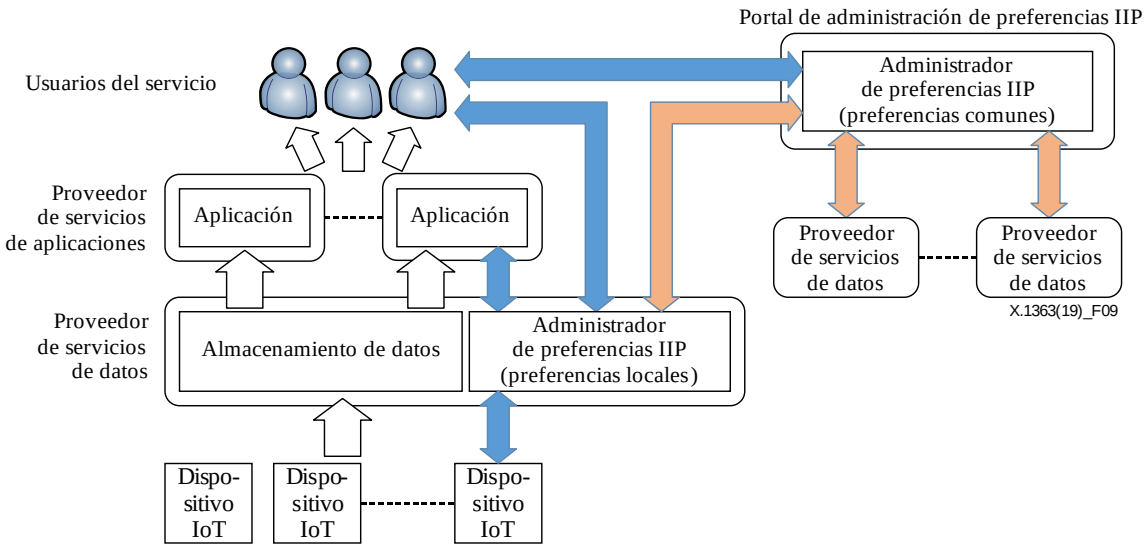

Figura 9 – Marco técnico para el tratamiento de datos IIP por múltiples proveedores de servicios con un portal común para la administración de preferencias IIP

Bibliografía

[b-UIT-T Y.4000] Recomendación UIT-T Y.4000/Y.2060, *Visión general de Internet de las cosas*.

[b-ISO/CEI 10027] ISO/CEI 10027:1990, *Information technology – Information Resource Dictionary System (IRDS) framework.*

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario*.

[b-ISO/TS 17975] ISO/TS 17975:2015, *Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information*.

[b-GAO-08-343] GAO-08-343 (2008). *Information security: Protecting personally identifiable information*. Washington, DC: United States Government Accountability Office. 34 pp.

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, 2020