ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1454 (09/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Aplicaciones y servicios con seguridad (2) – Seguridad de las aplicaciones (2)

Medidas de seguridad para servicios de oficina inteligente con ubicación activada

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	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
Comunicaciones de emergencia	X.1300-X.1309
Seguridad en las redes de sensores ubicuos	X.1310-X.1319
Seguridad en redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligentes (STI)	X.1370-X.1399
Seguridad en la tecnología de libro mayor distribuido (DLT)	X.1400-X.1429
Seguridad en las aplicaciones (2)	**X.1450-X.1459**
Seguridad en la web (2)	X.1470-X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

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

Recomendación UIT-T X.1454

Medidas de seguridad para servicios de oficina inteligente con ubicación activada

Resumen

Los servicios de oficina inteligente que combinan distintas aplicaciones inteligentes tienen como objetivo mejorar la calidad de la actividad empresarial de oficina y la eficacia de su gestión. Puesto que las tecnologías de la información y la comunicación (TIC) constituyen el núcleo de las tecnologías de los servicios de oficina inteligente, el operador de telecomunicaciones desempeña un importante papel de entre las partes interesadas en estos servicios.

Los servicios de oficina inteligente comprenden el estacionamiento inteligente, la conducción inteligente, las tiendas inteligentes, las propias oficinas inteligentes, la gestión inteligente de salas de reuniones, la gestión inteligente del consumo de agua y energía, etc. Entre los servicios más característicos de oficinas inteligentes, los datos de ubicación facilitados por el operador son uno de los elementos esenciales en la mayor parte de las instalaciones de estos servicios.

Con el fin de garantizar la seguridad de los servicios de oficina inteligente con ubicación activada, es necesario examinar los riesgos y requisitos de seguridad que guardan una relación específica con los servicios de ubicación, así como establecer medidas generales de seguridad adecuadas.

En la Recomendación UIT-T X.1454 se analizan las situaciones típicas de aplicación de los servicios de oficina inteligente con ubicación activada, se especifican los riesgos y requisitos de seguridad y se establecen las medidas de seguridad para el operador y para las partes interesadas más importantes de la oficina inteligente con el fin de proteger los servicios de ubicación.

Historia*

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T X.1454	2023-09-08	17	11.1002/1000/15111

Palabras clave

Medidas de seguridad, servicios de oficina inteligente, ubicación.

* Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 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.1454

Medidas de seguridad para servicios de oficina inteligente con ubicación activada

1 Cometido

En esta Recomendación se analizan las situaciones típicas de aplicación de los servicios de oficina inteligente con ubicación activada, se especifican los riesgos y requisitos de seguridad específicos de los servicios de ubicación activada y, de este modo, se establecen las medidas de seguridad para el operador y para las partes interesadas más importantes de la oficina inteligente para la salvaguarda de los servicios asociados a la posición.

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.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 servicio de oficina inteligente: Un servicio que combina múltiples aplicaciones inteligentes (por ejemplo, aparcamiento inteligente, gestión inteligente del agua, tienda inteligente, etc.) y que tiene como objetivo dar servicio y prestar asistencia a las actividades de oficina, mejorar su calidad y la eficiencia de su gestión, y crear un entorno de oficina adecuado para las personas.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

DDoS Denegación de servicio distribuida *(Distributed Denial of Service)*

GNSS Sistema mundial de navegación por satélite *(Global Navigation Satellite System)*

TIC Tecnologías de la información y la comunicación *(Information and Communication Technology)*

SRNA Sistema de radionavegación por satélite (*Radio Navigation Satellite System*)

SEM Supervisión medioambiental inteligente *(Smart Environmental Monitoring)*

UWB Banda ultra amplia *(Ultra-Wide Band)*

WiFi Fidelidad inalámbrica *(Wireless Fidelity)*

5 Convenios

La expresión "**se requiere**" indica un requisito que debe cumplirse estrictamente sin variación alguna para poder alegar la conformidad con este documento.

6 Generalidades sobre los servicios de oficina inteligente con ubicación activada

En armonía con la visión de las ciudades inteligentes y sostenibles, que aprovechan las tecnologías de la información y la comunicación (TIC) y otros medios para mejorar la calidad de vida, la eficiencia del funcionamiento y los servicios urbanos y la competitividad, los servicios de oficina inteligente se convierten en aplicaciones típicas de las ciudades inteligentes y sostenibles.

Los servicios de oficina inteligente, que combinan diversas aplicaciones inteligentes (por ejemplo, aparcamiento inteligente, gestión inteligente del agua, tiendas minoristas inteligentes, etc.), tienen por objeto mejorar la calidad de la actividad empresarial de oficina y la eficacia de su gestión.

Puesto que los servicios de oficina inteligente combinan diversas aplicaciones inteligentes, las partes interesadas clave son múltiples. Dado que las TIC constituyen el núcleo tecnológico de los servicios más característicos de oficina inteligente, los datos de ubicación facilitados por el operador constituyen uno de los principales elementos en la mayor parte de estos servicios.

Las principales partes interesadas en los sistemas de oficina inteligente con ubicación activada son:

– el proveedor de servicios de oficina inteligente;
– el proveedor de datos y servicios de computación;
– el proveedor de servicios de detección e infraestructuras;
– el usuario.

NOTA – Estas partes interesadas principales, a saber, el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación y el proveedor de servicios de detección e infraestructuras, en los sistemas de oficina inteligente con ubicación activada pueden ser proveedores separados o un solo proveedor de servicios integrados.

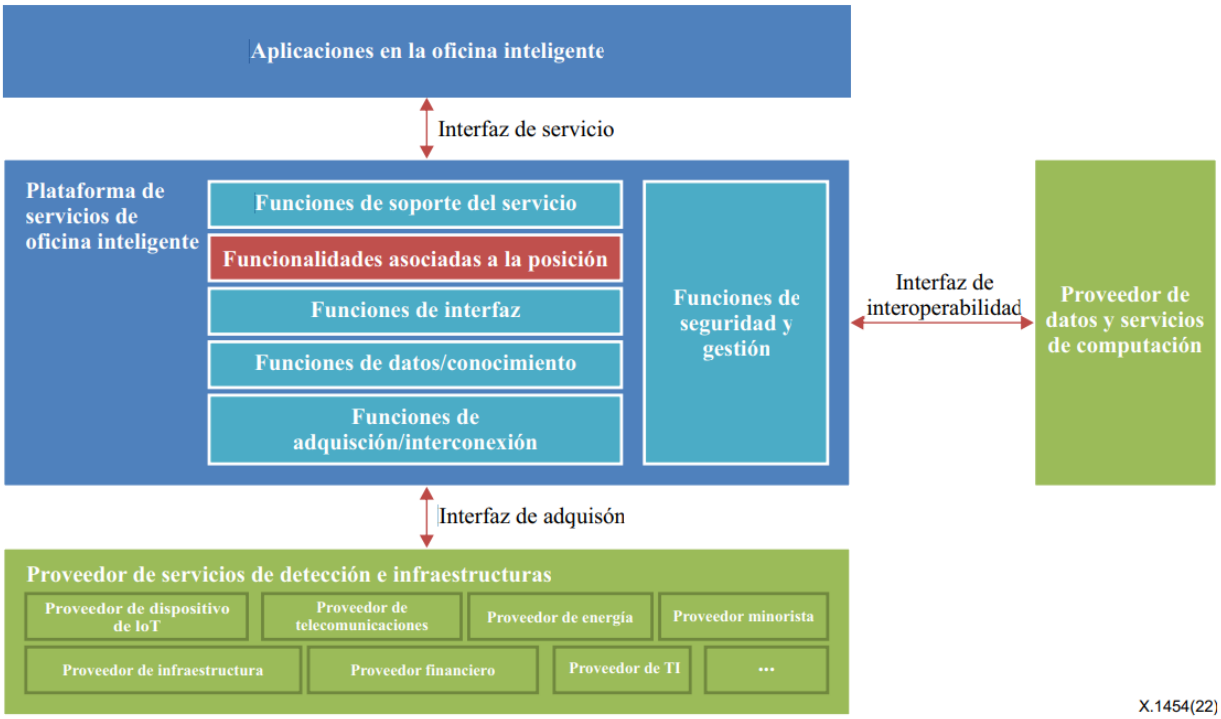

Figura 1 – Generalidades sobre los sistemas de oficina inteligente con ubicación activada

Un sistema de oficina inteligente con ubicación activada ofrece las siguientes funciones:

– **Funciones de adquisición/interconexión:** Ofrecen mecanismos de adquisición de datos a partir de diferentes sistemas de recopilación de datos.

– **Funciones de datos/conocimiento:** Asisten en el tratamiento de los datos mediante la adición de valor y la transformación de la información en conocimiento.

– **Funciones de interfaz:** Permiten el acceso a la información a distintos niveles.

– **Funciones asociadas a la posición:** Ofrecen datos de ubicación procedentes del sistema del operador.

– **Funciones de soporte del servicio:** Coordinan todos los servicios posibles que intervienen en cada acción y proporciona funciones de interoperabilidad.

– **Funciones de seguridad y gestión:** Brindan funcionalidades horizontales, como auditorías, supervisión y seguridad.

Las interfaces permiten la comunicación entre las funciones:

– **Interfaz de adquisición:** Esta interfaz permite la recogida de información procedente de elementos externos.

– **Interfaz de interoperabilidad:** Esta interfaz permite la comunicación con proveedores de datos externos y sistemas terceros de conmutación.

– **Interfaz de servicio:** Esta interfaz permite el acceso de aplicación a aplicación a funciones de soporte ofrecidas por la plataforma de los servicios de oficina inteligente.

7 Casos de aplicación típicos de los servicios de oficina inteligente con ubicación activada

7.1 Aparcamiento inteligente

El aparcamiento inteligente permite una integración eficaz de los recursos de aparcamiento en una oficina y coordina las instalaciones de estacionamiento con otros sistemas (por ejemplo, sistemas externos de pago, sistemas de aparcamiento en línea o por aplicación).

El aparcamiento inteligente puede incluir servicios típicos como la guía de estacionamiento, la reserva de plazas de estacionamiento, la búsqueda inversa de vehículos, el control de acceso automático a vehículos y el pago en autoservicio. Las modalidades de aparcamiento inteligente con ubicación activada son las siguientes:

– **Guía de estacionamiento:** Los datos de ubicación sobre plazas de estacionamiento no ocupadas permiten publicar información orientativa para aparcar.

– **Reserva de plazas de estacionamiento:** Los datos de ubicación pueden ayudar a buscar información sobre las plazas de estacionamiento disponibles y a reservarlas con antelación.

– **Búsqueda inversa de vehículos:** Los datos de ubicación pueden ayudar a los conductores a recordar dónde están estacionados sus vehículos en caso de que se les haya olvidado.

7.2 Supervisión medioambiental inteligente

Al igual que las aplicaciones de autosupervisión y de autoprotección medioambiental, la supervisión medioambiental inteligente (SEM, *Smart environmental monitoring*) puede mantenerse al corriente de las condiciones medioambientales actuales.

La SEM puede incluir entidades funcionales de plataformas y dispositivos SEM y de la red. Las modalidades de supervisión medioambiental inteligente con ubicación activada son las siguientes:

– **Gestión del ajuste de medición:** La ubicación de un dispositivo es un dato necesario para los ajustes de medición, junto con los factores medioambientales.

– **Presentación de datos:** Los datos en bruto en cada ubicación determinada (de uno o más dispositivos de SEM) constituyen información opcional para la presentación de la calidad medioambiental.

7.3 Suministro inteligente

El suministro inteligente se beneficia de las aplicaciones de robótica y vehículos autónomos en situaciones de oficina inteligente, y permite entregar de forma automática paquetes, archivos, artículos de oficina, etc.

Las modalidades de suministro inteligente con ubicación activada son las siguientes:

– asistencia a la conducción automática mediante las capacidades de posicionamiento con precisión centimétrica;

– mejora de la eficacia de los envíos con robots/vehículos mediante la correlación del pedido con la ubicación del dispositivo;

– optimización de la ruta de suministro y supervisión del proceso de entrega mediante el seguimiento en tiempo real de la ubicación del vehículo/robot.

8 Riesgos de seguridad para los servicios de oficina inteligente con ubicación activada

8.1 Riesgos de seguridad para los datos

8.1.1 Interceptación de datos de ubicación

Los datos de ubicación en los servicios de oficina inteligente pueden estar basados en la red inalámbrica abierta, por lo que un atacante podría interceptarlos supervisando el canal inalámbrico.

8.1.2 Manipulación de datos de ubicación

El atacante podría capturar el paquete de datos con los datos de ubicación transmitidos desde la red y modificarlos o falsearlos con fines perniciosos para iniciar ataques posteriores. En ciertas situaciones, los datos modificados o falseados de ubicación pueden causar problemas de seguridad, por ejemplo, en el caso del aparcamiento inteligente, la conducción inteligente y el rescate de emergencia.

8.1.3 Intercepción de la comunicación de los datos de ubicación

El atacante podría capturar o manipular los dispositivos de IoT y negarse a comunicar los datos de ubicación de los mismos a la red o a la plataforma de los servicios de oficina inteligente.

8.1.4 Invocación no autorizada de los datos de ubicación

Sin un mecanismo de autentificación entre las aplicaciones y la plataforma de los servicios de oficina inteligente, puede ocurrir que el atacante invoque sin autorización los datos de ubicación.

8.1.5 Indisponibilidad de los datos

Un formato no unificado de datos puede dar lugar a que la aplicación esté indisponible en una oficina inteligente. Por ejemplo, el formato no unificado de datos de ubicación interior (incluidos los relativos al piso, la sala o el escritorio) puede confundir al robot que entrega un paquete a su destinatario.

8.1.6 Revelación de información sobre la conducta

Este riesgo se da cuando se manipula la plataforma de oficina inteligente o cuando el atacante usurpa la identidad de una entidad legítima y aprovechan la ocasión para hacerse con datos sobre la conducta de los usuarios (por ejemplo, preferencias de planificación de rutas) con fines perniciosos, como su venta para obtener beneficios.

8.1.7 Ubicación sin el consentimiento del usuario

Este riesgo se da cuando la entidad que brinda la función de ubicación utiliza los datos de ubicación del usuario y analiza los datos conexos sin el consentimiento del usuario, en particular el cometido, la intención, el método, el uso de resultados, etc.

8.2 Riesgos de seguridad para el dispositivo

8.2.1 Vulnerabilidad de *hardware* y *software*

Pueden aparecer vulnerabilidades y riesgos de seguridad en el proceso de desarrollo de los dispositivos de posicionamiento. Por ejemplo, es posible que los puertos destinados a actividades de depuración no estén protegidos adecuadamente, que se hayan utilizado algoritmos de cifrado poco eficaces, que se haya producido un fallo al actualizar el *hardware* y el *software* y que no se haya llevado a cabo a tiempo una comprobación de integridad.

8.2.2 Manipulación del dispositivo de posicionamiento

El atacante podría manipular el dispositivo de posicionamiento interviniendo en los sistemas de detección e infraestructura, lo que podría generar un resultado de posicionamiento impreciso.

8.3 Riesgos de seguridad para las interfaces

8.3.1 Interfaz de adquisición

La interfaz entre el proveedor de los servicios de detección e infraestructuras y los servicios de oficina inteligente es vulnerable a los siguientes riesgos:

– **Intercepción de datos:** Si no hay mecanismos de autentificación y autorización entre la plataforma de servicios de oficina inteligente y el proveedor de servicios de detección e infraestructura, el atacante podría usurpar la identidad de la plataforma de servicios de oficina inteligente para hacerse con los datos de detección e infraestructura.

– **Denegación del servicio:** El atacante podría lanzar ataques de denegación de servicio distribuida (DDoS) modificando la política de recogida de datos (por ejemplo, recogiendo frecuentemente los datos de detección e infraestructura en un periodo de tiempo muy breve).

– **Fugas de información:** Los dispositivos móviles envían periódicamente datos de servicio, sobre todo datos de ubicación, a través de la interfaz de adquisición a la plataforma de servicios de oficina inteligente. Si el atacante tiene la posibilidad de inspeccionar los datos de servicio y ubicación, podría detectar la rutina cotidiana del usuario.

8.3.2 Interfaz de interoperabilidad

La interfaz entre la plataforma de servicios de oficina inteligente y el proveedor de datos/servicios de computación es vulnerable a los siguientes riesgos:

– **Acceso no autorizado a los datos:** Si no hay mecanismos de autentificación y autorización entre la plataforma de servicios de oficina inteligente y el proveedor de datos/servicios de computación, el atacante podría manipular la interfaz de interoperabilidad para acceder a los datos de servicio, de ubicación y de perfiles.

– **Falsificación de datos:** Si no hay mecanismos de autentificación y autorización entre la plataforma de servicios de oficina inteligente y el proveedor de datos/servicios de computación, el atacante podría manipular la interfaz de interoperabilidad para falsificar los datos de servicio, de ubicación y de perfiles; este riesgo podría provocar una fuga de información, un funcionamiento incorrecto de la plataforma y una emisión errónea de facturas al proveedor de datos/servicios de computación.

8.3.3 Interfaz de servicio

La interfaz entre la plataforma de servicios de oficina inteligente y las aplicaciones en la oficina inteligente es vulnerable a los siguientes riesgos:

– **Acceso no autorizado a los datos:** Si no hay mecanismos de autentificación y autorización entre la plataforma de servicios de oficina inteligente y las aplicaciones en la oficina inteligente, el atacante podría manipular la interfaz de servicio para acceder a los datos de servicio, de ubicación y de perfiles.

– **Falsificación de datos:** Si no hay mecanismos de autentificación y autorización entre la plataforma de servicios de oficina inteligente y las aplicaciones en la oficina inteligente, el atacante podría manipular la interfaz de servicio para falsificar los datos de servicio, de ubicación y de perfiles; este riesgo podría provocar una emisión errónea de facturas a los clientes.

8.4 Riesgos de seguridad para la plataforma

8.4.1 Vulnerabilidad de las tecnologías de localización híbridas

Es posible que la función de localización, como una de las entidades funcionales básicas de la capa de plataforma, tenga que agregar tecnologías de localización híbridas basadas en diversos sistemas inalámbricos como GPS, Bluetooth, WiFi, redes celulares, banda ultra amplia (UWB), etc. La

aplicación de estas tecnologías de localización híbridas supone la extracción de información, el cálculo del posicionamiento y el filtrado de la vulnerabilidad del proceso de agregación, por lo que el algoritmo puede generar un resultado de posicionamiento impreciso.

8.4.2 Exposición de capacidades

La plataforma de servicios de oficina inteligente expone las capacidades de ubicación y otros servicios a las aplicaciones inteligentes, por lo que una entidad no autorizada podría introducir, modificar o eliminar privilegios de uso de dichas capacidades. La entidad no autorizada puede ser una persona, un programa o un dispositivo. Estos ataques se producen cuando un atacante agrega datos a una conexión existente teniendo la capacidad de servicio de apoderarse de la misma o de enviar datos de configuración con fines perniciosos. Como resultado, pueden producirse ataques de denegación del servicio y accesos a los datos de servicio.

8.5 Riesgos de seguridad para las aplicaciones inteligentes

8.5.1 Uso no autorizado

Este riesgo se da cuando una aplicación inteligente no autorizada se hace con capacidades de servicio ofrecidas por una plataforma de oficina inteligente, haciéndose pasar por una entidad autorizada.

8.5.2 Introducción de virus y troyanos

Se produce cuando un atacante usurpa la identidad de una aplicación inteligente lícita e introduce un troyano o un virus en la aplicación inteligente, capaz de dañar e incluso de continuar atacando la plataforma de la oficina inteligente.

8.6 Relación entre los riesgos de seguridad y las principales partes interesadas

En el Cuadro 1 se indica la relación entre los riesgos de seguridad y las principales partes interesadas en los servicios de oficina inteligente con ubicación activada.

En el Cuadro 1, la letra "S" ("sí") en cada celda indica que la parte interesada principal está relacionada con un riesgo de seguridad específico.

Cuadro 1 – Relación de los riesgos de seguridad para cada entidad

Parte interesada principal / **Riesgos**	**Proveedor de servicios de oficina inteligente**	**Proveedor de datos y servicios de computación**	**Proveedor de servicios de detección e infraestructuras**	**Usuario**
Interceptación de datos de ubicación	S		S	S
Manipulación de datos de ubicación	S		S	S
Interrupción de la comunicación de los datos de ubicación	S		S	S
Invocación no autorizada de los datos de ubicación	S		S	S
Indisponibilidad de los datos	S	S		
Revelación de información sobre la conducta	S	S	S	S

Cuadro 1 – Relación de los riesgos de seguridad para cada entidad

Parte interesada principal / Riesgos	Proveedor de servicios de oficina inteligente	Proveedor de datos y servicios de computación	Proveedor de servicios de detección e infraestructuras	Usuario
Posicionamiento sin el consentimiento del usuario	S		S	S
Intercepción de datos	S		S	S
Denegación del servicio	S		S	
Fugas de información	S		S	S
Acceso no autorizado a los datos	S	S	S	S
Falsificación de datos	S	S	S	S
Vulnerabilidad de las tecnologías de localización híbridas			S	
Exposición de capacidades	S			
Vulnerabilidad de *hardware* y *softwar*e			S	
Manipulación del dispositivo de posicionamiento			S	
Uso no autorizado	S			
Introducción de virus y troyanos	S			

9 Requisitos de seguridad para los servicios de oficina inteligente con ubicación activada

9.1 Requisitos de seguridad para los datos

– R-01: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura proporcionen una funcionalidad que garantice la confidencialidad de los datos, especialmente de los datos de localización.

– R-02: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios detección e infraestructura proporcionen una funcionalidad para garantizar la integridad de los datos, especialmente los datos de localización.

– R-03: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura garanticen que sólo los usuarios o dispositivos autorizados puedan acceder a los datos, especialmente a los datos de localización.

– R-04: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura confirmen la identidad de las entidades e impidan que los atacantes intenten hacerse pasar por una entidad autorizada.

– R-05: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad que garantice que sólo los dispositivos o aplicaciones autorizados puedan acceder al entorno de la oficina.

– R-06: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y de servicios de computación, y el proveedor de servicios de detección e infraestructura establezcan un mecanismo de colaboración para unificar el formato de los datos.

– R-07: Es necesario que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura estén autorizados por medio del consentimiento del usuario a recopilar los datos personales de los usuarios, especialmente los datos de ubicación. El consentimiento del usuario incluye el consentimiento para que se le recuerde, se le muestre y se le explique brevemente la recopilación de sus datos personales.

En cuanto a los datos del servicio de oficina inteligente con ubicación activada, en el Cuadro 2 se muestran los requisitos de seguridad correspondientes a cada riesgo para la seguridad.

Cuadro 2 – Relación entre los requisitos de seguridad de los datos y los riesgos de seguridad

Riesgos de seguridad	Requisitos de seguridad
Interceptación de datos de ubicación	R-01, R-02, R-03, R-04
Manipulación de datos de ubicación	R-03, R-04
Intercepción de la comunicación de los datos de ubicación	R-03, R-04
Invocación no autorizada de los datos de ubicación	R-03, R-04, R-05
Indisponibilidad de los d	R-06
Revelación de información sobre la conducta	R-01, R-03, R-04
Ubicación sin el consentimiento del usuario	R-07

9.2 Requisitos de seguridad para el dispositivo

– R-08: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura proporcionen un mecanismo de respuesta a incidentes para la detección de *malware*, que desplieguen de antemano mecanismos de seguridad contra ataques y respondan a tiempo a los ataques.

– R-09: Se requiere que el proveedor de sensores e infraestructura garantice que el atacante no pueda acceder a los datos aun cuando el *hardware* haya sido secuestrado, lo que incluye lo siguiente:

  • Verificar la autenticidad e integridad del *software* del dispositivo utilizando firmas digitales generadas criptográficamente. [b-ISO/IEC 9796-3];

  • Controlar el tráfico cuyo destino final sea el dispositivo por medio de cortafuegos y mecanismos de detección y protección contra intrusiones.

– R-10: Se requiere que el proveedor de servicios de oficina inteligente, el proveedor de datos y servicios de computación, y el proveedor de servicios de detección e infraestructura utilicen algoritmos de encriptado adecuados para garantizar la confidencialidad de los datos, especialmente de los datos de ubicación.

– R-11: Se requiere que el proveedor de detección e infraestructura proporcione una funcionalidad para confirmar las identidades de las entidades e impedir que cualquier atacante intente hacerse pasar por una entidad autorizada.

En cuanto a los dispositivos del servicio de oficina inteligente con ubicación activada, en el Cuadro 3 se muestra los requisitos de seguridad correspondientes a cada riesgo para la seguridad.

Cuadro 3 – Relación entre los requisitos de seguridad de los dispositivos y los riesgos de seguridad

Riesgos de seguridad	Requisitos de seguridad
Vulnerabilidad del *hardware* y del *software*	R-08, R-09, R-10
Manipulación del dispositivo de posicionamiento	R-09, R-11

9.3 Requisitos de seguridad para las interfaces

– R-12: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de servicios de detección e infraestructura proporcionen una funcionalidad que garantice que sólo los usuarios o dispositivos autorizados puedan acceder a los datos de detección e infraestructura a través de las interfaces.

– R-13: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de servicios de detección e infraestructura proporcionen una funcionalidad para confirmar las identidades de las entidades e impedir que cualquier atacante intente hacerse pasar por una entidad autorizada.

– R-14: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de servicios de detección e infraestructura proporcionen una funcionalidad que garantice la confidencialidad de los datos, especialmente de los datos de ubicación.

– R-15: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de datos y servicios de computación proporcionen una funcionalidad que garantice que sólo los usuarios autorizados puedan acceder a los datos de servicio, los datos de ubicación y los datos de perfil.

– R-16: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de servicios de datos y computación proporcionen una funcionalidad para confirmar las identidades de las entidades e impedir que cualquier atacante intente hacerse pasar por una entidad autorizada.

– R-17: Se requiere que el proveedor de servicios de oficina inteligente y el proveedor de datos y servicios de computación proporcionen una funcionalidad que garantice la integridad de los datos del servicio, los datos de ubicación y los datos de perfil.

En cuanto a la interfaz del servicio de oficina inteligente con ubicación activada, en el Cuadro 4 se muestra los requisitos de seguridad correspondientes a cada riesgo para la seguridad.

Table 4 – Relación entre los requisitos de seguridad de las interfaces y los riesgos de seguridad

Riesgo de seguridad	Requisitos de seguridad
Sniff data	R-12, R-13
Denegación del servicio	R-13
Fugas de información	R-13, R-14
Acceso no autorizado a los datos	R-15, R-16
Falsificación de datos	R-17

9.4 Requisitos de seguridad para la plataforma

– R-18: Se requiere que el proveedor de detección e infraestructura proporcione una funcionalidad para comprobar la exactitud e integridad del algoritmo o algoritmos de ubicación híbridos.

– R-19: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad que garantice que sólo los dispositivos o aplicaciones autorizados puedan acceder al servicio de oficina inteligente con ubicación activada.

– R-20: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad para confirmar las identidades de las entidades e impedir que cualquier atacante intente hacerse pasar por una entidad autorizada.

En cuanto a la plataforma del servicio de oficina inteligente con ubicación activada, en el Cuadro 5 se muestran los requisitos de seguridad correspondientes a cada riesgo para la seguridad.

Table 5 – Relación entre los requisitos de seguridad de la plataforma y los riesgos de seguridad

Riesgo de seguridad	Requisitos de seguridad
Vulnerabilidad de las tecnologías de ubicación híbridas	R-18
Exposición de capacidad	R-19, R-20

9.5 Requisitos de seguridad para la aplicación inteligente

– R-21: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad que garantice que sólo los usuarios o dispositivos autorizados puedan acceder a los datos, especialmente a los datos de ubicación.

– R-22: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad que garantice que sólo los dispositivos o aplicaciones autorizados puedan acceder al servicio de oficina inteligente.

– R-23: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad que garantice que sólo los usuarios o dispositivos autorizados puedan acceder al servicio de oficina inteligente con ubicación activada.

– R-24: Se requiere que el proveedor de servicios de oficina inteligente proporcione una funcionalidad para activar un proceso de respuesta a incidentes de detección de *malware*, para desplegar de antemano mecanismos de seguridad contra ataques y atajarlos a tiempo.

En cuanto a la aplicación inteligente del servicio de oficina inteligente con ubicación activada, en el Cuadro 6 se muestran los requisitos de seguridad correspondientes a cada riesgo para la seguridad.

Cuadro 6 – Relación entre los requisitos de seguridad de la aplicación inteligente y los riesgos de seguridad

Riesgos de seguridad	Requisitos de seguridad
Utilización no autorizada	R-21, R-22
Inyección de virus y troyanos	R-23, R-24

10 Funciones de seguridad

Para cumplir con los requisitos de seguridad de los servicios de oficina inteligente con ubicación activada existen diversas funciones de seguridad, entre las que se encuentran las siguientes:

– encriptación de datos y gestión de claves;
– gestión de la identidad y control de acceso;
– verificación de la integridad;
– supervisión de la seguridad y respuesta a eventos de seguridad;
– recordatorios del usuario.

10.1 Encriptación de datos y gestión de claves

La encriptación y la gestión de claves son los mecanismos principales para proteger la confidencialidad de los datos en los servicios de oficina inteligente. La encriptación permite la protección de los recursos, mientras que la gestión de claves brinda el control de las claves criptográficas.

La encriptación debe seguir las normas gubernamentales y del sector pertinentes. Incluye, entre otros, los elementos siguientes:

– encriptación de datos dinámicos en procesos de servicio;
– encriptación de datos estáticos en la base de datos;
– encriptación de datos en el fichero de copia de seguridad.

La gestión de claves abarca la generación, la distribución, la difusión, la actualización y la revocación de claves criptográficas para la confidencialidad de los datos y la autentificación. La gestión conforma los cimientos de la seguridad del servicio, que incluye, entre otros, los siguientes elementos:

– **Protección de información de claves:** la información de claves debe protegerse como datos sensibles y su nivel de seguridad debe ser mayor que el que se aplica a otros elementos.
– **Copias de seguridad y recuperación:** Dado que un potencial incidente podría provocar la pérdida de una clave específica e interrumpir un servicio, es esencial configurar una solución de copia de seguridad y recuperación de la clave.

10.2 Gestión de la identidad y control de acceso

Las entidades de servicios de oficina inteligente que pueden suministrar datos brutos de control de acceso, autorización y auditoría deberían disponer de un sistema de gestión de la identidad.

– Soporta el control de la identidad durante toda la vida útil, por ejemplo, el registro, la asignación de la función y de los permisos, la modificación y eliminación de permisos. Además, el registro y la modificación de la identidad debe someterse a un procedimiento de aprobación por el administrador.
– Soporta la gestión de las contraseñas de la entidad, lo que incluye el conjunto de políticas de contraseñas de la entidad con arreglo a la política de seguridad del cliente, como los algoritmos criptográficos, la longitud de la contraseña, su complejidad o su ciclo de actualización. Tendría que poder ser compatible con distintos tipos de contraseñas, como las gráficas o sonoras, entre otras. Además, soporta también las funciones de sincronización y de renovación de las contraseñas.
– La gestión de la identidad debería incluir la política de denominación de la cuenta de la identidad y la política de aplicación de la cuenta de la identidad.

Debería facilitarse un control de acceso para gestionar el acceso de la entidad a los servicios de oficina inteligente, que utilice la identidad autentificada de una entidad o las capacidades de la misma para determinar y aplicar los derechos de acceso de la entidad. El control de acceso puede denegar los intentos de acceso no autorizados o inapropiados y comunicarlos para generar una alarma o una pista de auditoría de seguridad.

– Los datos de autentificación, como las contraseñas, su posesión y su presentación ulterior, son la prueba de la autorización del acceso de la entidad.

– La etiqueta de seguridad se genera de acuerdo con la política de seguridad de la oficina.
– Hora del intento de acceso.
– Ruta del intento de acceso.
– Duración del acceso.
– Ubicación física del intento de acceso.

10.3 Verificación de la integridad

La verificación de la integridad de los datos consta de dos niveles:

– **Nivel individual de campo o unidad de datos:** La verificación de la integridad de un nivel individual de unidad de datos entraña dos procesos, uno en la entidad expedidora y otro en la entidad receptora. La entidad expedidora añade a los datos una cantidad que es una función de los propios datos. La entidad receptora genera una cantidad correspondiente y compara su resultado con la cantidad recibida para determinar si los datos han sido modificados en tránsito.
– **Nivel de tren de campos o unidades de datos:** La verificación del nivel de tren de unidades de datos requiere la incorporación de cierto método de ordenamiento explícito, por ejemplo, secuencia numérica, sello temporal o cadena criptográfica.

Verificación de la integridad de los datos mediante un mecanismo de despliegue previo para verificar el formato de los datos y un mecanismo de firma digital generado criptográficamente para verificar que los datos no hayan sido alterados.

10.4 Verificación de la integridad del *software* y el algoritmo o los algoritmos mediante un mecanismo de firmas digitales criptográficamente generadas – Supervisión de la seguridad y respuesta a eventos de seguridad

Puede facilitarse un sistema de supervisión de la seguridad a los administradores de sistemas para inspeccionar fallos de servicio y rendimiento. La supervisión incluye, entre otros, los elementos siguientes:

– **Vigilancia del estado:** Incluye la recopilación y la visualización del registro de eventos de seguridad, la información sobre vulnerabilidad, la alteración de la configuración de dispositivos de seguridad y el estado operativo y de rendimiento en servicio. Ayuda a los administradores a ser conscientes del estado general del servicio.
– **Detección de comportamientos anormales:** Incluye las conexiones ilícitas, los accesos ilícitos o las violaciones del acceso a servicios específicos, así como las modificaciones anómalas de un dispositivo físico.
– **Vigilancia de la seguridad física:** Incluye el control de la temperatura y la humedad, la televisión en circuito cerrado (CCTV), la vigilancia de seguridad en los accesos, un sistema de protección contra incendios, el aire acondicionado, el sistema de alimentación de energía y la supervisión.

La respuesta a eventos de seguridad trata las peticiones y conlleva la recuperación de mecanismos tales como las funciones de tratamiento y gestión de los eventos, y realiza acciones de recuperación como resultado de la aplicación de un conjunto de reglas.

10.5 Recordatorio al usuario

El recordatorio al usuario constituye un mecanismo para garantizar que los datos recabados del dispositivo sensor se van a utilizar y que el usuario de los servicios de oficina inteligente con ubicación activada ha autorizado dicha utilización.

Lo fundamental es que, para un determinado servicio de oficina inteligente con ubicación activada que deba recopilar datos del usuario, el servicio envíe un recordatorio al usuario, se lo muestre y se lo explique brevemente. Se podrá recordar al usuario qué datos se ha previsto recopilar. También se le informará de cómo se procesarán y tratarán los datos.

10.6 Relación entre la función de seguridad y los requisitos de seguridad

En el Cuadro 7 figuran las funciones de seguridad necesarias para cumplir los requisitos de seguridad correspondientes para un servicio inteligente con ubicación activada.

Cuadro 7 – Relación entre los requisitos de seguridad y las funciones de seguridad

Funciones de seguridad	**Requisitos de seguridad**	
Encriptación de datos y gestión de claves	Para los datos: R-01	
	Requisitos de seguridad para el dispositivo	R-09, R-10, R-11
	Requisitos de seguridad para las interfaces	R-14
Gestión de identidades y control de acceso	Requisitos de seguridad para los datos	R-03, R-04, R-05
	Requisitos de seguridad para las interfaces	R-12, R-13, R-15, R-16
	Requisitos de seguridad para la plataforma	R-19, R-20
	Requisitos de seguridad para la aplicación inteligente	R-21, R-22, R-23
Verificación de la integridad	Requisitos de seguridad para los datos	R-02, R-06
	Requisitos de seguridad para las interfaces	R-17
	Requisitos de seguridad para la plataforma	R-18
Supervisión de la seguridad y respuesta a eventos de seguridad	Requisitos de seguridad para el dispositivo	R-08, R-09
	Requisitos de seguridad para la aplicación inteligente	R-24
Recordatorio al usuario	Requisitos de seguridad para los datos	R-07

Bibliografía

[b-ITU-T X.1121] Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.

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

Publicado en Suiza
Ginebra, 2024