ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1383 (03/2023)

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

Aplicaciones y servicios seguros (2) – Seguridad de los sistemas de transporte inteligentes (STI)

Requisitos de seguridad para los datos categorizados en la comunicación entre el vehículo y su entorno (V2X)

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	
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 (1)	X.1140–X.1149
Seguridad de aplicación (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.1319
Seguridad de las redes eléctricas	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 inteligente (ITS)	**X.1370–X.1399**
Seguridad de tecnología de libro mayor distribuido (DTL)	X.1400–X.1429
Seguridad de aplicaciones (2)	X.1450–X.1459
Seguridad de web (2)	X.1470–X.1489
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
Ciberdefensa	X.1590–X.1599
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	
Terminología	X.1700–X.1701
Generador de número 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 DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1383

Requisitos de seguridad para los datos categorizados en la comunicación entre el vehículo y su entorno (V2X)

Resumen

La seguridad de los datos es una de las consideraciones más importantes para la comunicación del vehículo con su entorno (V2X). Sin embargo, en un entorno con recursos limitados como la comunicación a bordo de un vehículo, la protección de los datos consume muchos recursos, ya que se requieren funciones criptográficas.

En la Recomendación UIT-T X.1383 se clasifican los datos utilizados en la comunicación V2X de varios tipos, como los datos de atributos de los objetos, los datos de estado del vehículo, los datos de percepción del entorno, los datos de control del vehículo, los datos de servicio de la aplicación y los datos personales del usuario, y se asignan tres niveles de seguridad para los tipos de datos categorizados. Sobre la base de estos tipos de datos categorizados y de los niveles asignados de seguridad de datos, en la presente Recomendación se establecen los requisitos de seguridad para los datos categorizados en la comunicación V2X.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1383	03-03-2023	17	11.1002/1000/15108

Palabras clave

Comunicación V2X, datos categorizados, seguridad de los datos.

* 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.1383

Requisitos de seguridad para los datos categorizados en la comunicación entre el vehículo y su entorno (V2X)

1 Alcance

En la presente Recomendación se clasifican los datos utilizados en la comunicación del vehículo con su entorno (V2X) de varios tipos y se define el nivel de seguridad para cada tipo de datos categorizado. Sobre la base de estos tipos de datos categorizados en cada nivel de seguridad, en la presente Recomendación se establecen los requisitos de seguridad para los datos categorizados en la comunicación V2X.

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. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T X.1372] Recomendación UIT-T X.1372 (2020), *Directrices de seguridad para la comunicación entre el vehículo y su entorno (V2X).*

[UIT-T X.1603] Recomendación UIT-T X.1603 (2018), *Requisitos de seguridad de los datos para el servicio de control de la computación en la nube.*

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

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 desensibilización de datos [b-UIT-T X.1217]: Proceso para ocultar los datos sensibles.

3.1.2 ciclo de vida de los datos [b-UIT-T X.1751]: Todo el proceso de supervivencia después de que se generan, comprendida su recopilación, transmisión, almacenamiento, utilización (que comprende su análisis y visualización), intercambio y destrucción.

4 Abreviaturas y siglas

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

ABS Sistema de frenado antideslizante (*anti-skid braking system*)

BSM Mensaje básico de seguridad (*basic safety message*)

CAM Mensaje de sensibilización cooperativa (*cooperative awareness message*)

DoS Denegación de servicio (*denial of service*)

ICV Vehículo inteligente conectado (*intelligent connected vehicle*)

RGPD Reglamento General de Protección de Datos

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

V2D Dispositivo de vehículo a nómada (*vehicle-to-nomadic device*)

V2I Vehículo a infraestructura (*vehicle-to-infrastructure*)

V2P Vehículo a peatón (*vehicle-to-pedestrian*)

V2V Vehículo a vehículo (*vehicle-to-vehicle*)

V2X Vehículo a su entorno (*vehicle-to-everything*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

La expresión "**se requiere**" indica un requisito que debe cumplirse estrictamente, sin permitir desviación alguna si se va a invocar la conformidad con la presente Recomendación.

La utilización de las expresiones "**se recomienda/se ha de/se debe**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Por tanto, el cumplimiento de ese requisito no es necesario para invocar la conformidad.

La palabra "**puede**" indica un requisito opcional admisible que no reviste en absoluto el carácter de recomendación.

La expresión "**no debería**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si se va a invocar la conformidad con la presente Recomendación.

6 Ciclo de vida de los datos en la comunicación V2X

6.1 Ciclo de vida de los datos

El ciclo de vida de los datos se define en función del flujo de datos de la organización o empresa de que se trate en un entorno de comunicación entre el vehículo y su entorno (V2X). Basándose en la situación real de la comunicación V2X, el ciclo de vida de la seguridad de los datos es similar al presentado en [UIT-T X.1641], que incluye las etapas descritas a continuación de recogida de datos, transmisión de datos, almacenamiento de datos, uso de datos, migración de datos, destrucción de datos y copia de seguridad y restauración de datos:

– **Recopilación de datos**: Proceso de generación de nuevos datos en el sistema interno de la organización y de recogida de datos del exterior. Hay dos formas de recopilación de datos en la comunicación V2X: una es la generación de datos en diversos procesos empresariales de comunicación V2X y la otra es la recogida de datos recopilados por usuarios, asociados y demás terceros conexos.

– **Transmisión de datos**: Proceso en el que los datos fluyen de una entidad a otra dentro de la organización. La transmisión de datos en la comunicación V2X consiste principalmente en la realización del flujo de datos entre sistemas y equipos relacionados con los servicios de comunicación V2X.

– **Almacenamiento de datos**: Proceso de almacenamiento de datos en un soporte físico o en la nube en cualquier formato digital. Esta etapa suele ser casi simultánea a la recogida de datos.

– **Uso de datos**: Una serie de actividades realizadas por las organizaciones con respecto a los datos dinámicos en la comunicación V2X, como la consulta, el análisis y el tratamiento de datos. En esta etapa se procederá a la actualización de datos y a la producción de nuevos datos.

– **Migración de datos**: Proceso de transferencia de datos a terceros externos. Incluye la visualización y el suministro de datos a los usuarios en la comunicación V2X. También incluye el proceso de suministro de datos entre empresas e instituciones en la comunicación V2X.

– **Destrucción de datos**: Proceso para hacer que los datos no estén disponibles de forma permanente o temporal utilizando medios físicos o técnicos. La destrucción de datos puede deberse tanto a consideraciones de costos de la empresa como a requisitos externos de cumplimiento o de negocio. En particular, si existen disposiciones reglamentarias de conservación de datos relevantes, se recomienda considerar que los proveedores de servicios borren o anonimicen los datos recogidos de manera apropiada para que los datos que han alcanzado su límite de conservación o respecto de los cuales los usuarios ya no han dado su consentimiento no puedan ser recuperados.

– **Copia de seguridad y restauración de datos**: Proceso de copia de la totalidad o parte de los datos a otro medio de almacenamiento para evitar la pérdida de datos y para recuperar los datos originales con los de la copia de seguridad en caso de pérdida de datos.

6.2 Análisis de amenazas

En la comunicación V2X los datos también han de hacer frente a amenazas y problemas de seguridad similares a los definidos en [UIT-T X.1603] y [UIT-T X.1641]. Algunas de estas amenazas y problemas que afectan a la seguridad de los datos en la comunicación V2X se recogen en el Cuadro 6-1, si bien la lista no es exhaustiva.

Cuadro 6-1 – Amenazas y problemas según el ciclo de vida de los datos en la comunicación V2X

Ciclo de vida de los datos	Amenazas y problemas de seguridad
Recogida de datos	a) Recopilación de datos sin autorización b) Vulnerabilidades en interfaz de adquisición c) Robo de identidad d) Manipulación e intercepción e) Acceso inseguro al servicio f) Acceso con derechos de administración no autorizado
Transmisión de datos	a) Interceptación b) Suplantación de identidad c) Escucha furtiva d) Acceso no autorizado e) Ataque de denegación del servicio (DoS)
Almacenamiento de datos	a) Pérdida y filtración de datos b) Indisponibilidad de servicio
Uso de datos	a) Utilización indebida de datos b) Amenazas internas c) Vulnerabilidades del sistema d) Escucha furtiva
Migración de datos	a) Utilización indebida de datos b) Vulnerabilidades del sistema c) Interpretación inadecuada d) Ataque DoS

Cuadro 6-1 – Amenazas y problemas según el ciclo de vida de los datos en la comunicación V2X

Ciclo de vida de los datos	Amenazas y problemas de seguridad
Destrucción de datos	a) Robo de identidad b) Vulnerabilidades del sistema
Copia de seguridad y restauración de datos	a) Vulnerabilidades del sistema

7 Datos categorizados en las comunicaciones V2X

En esta cláusula se presenta la política de categorización de los datos tratados por la comunicación V2X. Las seis categorías de datos –datos de atributos de objeto, datos de estado del vehículo, datos de percepción del entorno, datos de control del vehículo, datos de servicio de la aplicación y datos personales del usuario– se describen en la cláusula 7.2.

7.1 Identificación de datos basada en escenarios de comunicación V2X

Los datos tratados por la comunicación V2X pueden identificarse sobre la base de un escenario de comunicación real. En [UIT-T X.1372] se clasifican los escenarios de comunicación V2X de la siguiente manera: de vehículo a vehículo (V2V), de vehículo a infraestructura (V2I), de vehículo a dispositivo nómada (V2D) y de vehículo a peatón (V2P). En la presente cláusula se describen los procesos de comunicación y los datos relevantes de cada escenario de comunicación.

7.1.1 Datos en la comunicación V2V

En [UIT-T X.1372] se identifican tres escenarios de comunicación V2V: propagación de alertas por V2V, comunicación en pelotón por V2V y balizaje por V2V. En un escenario de propagación de alertas por V2V, se propaga un mensaje de alerta entre vehículos. En un escenario de comunicación en pelotón por V2V, los grupos de vehículos intercambian el estado del vehículo entre sí. En un escenario de balizaje por V2V, cada vehículo envía su información de estado. En el Cuadro 7-1 se muestran los datos de la comunicación V2V.

Cuadro 7-1 – Datos en la comunicación V2V

Categoría	Escenario	Datos
De vehículo a vehículo (V2V)	Propagación de alertas por V2V	• Mensaje de alerta • Mensaje básico de seguridad (BSM) • Mensaje de sensibilización cooperativa (CAM)
	Comunicación en pelotón por V2V	• BSM • CAM
	Balizaje por V2V	• BSM • CAM

Las especificaciones técnicas de BSM y CAM se describen en [b-SAE J2735] y [b-ETSI TS 102 637-2], respectivamente.

7.1.2 Datos en la comunicación V2I

En [UIT-T X.1372] se identifican dos escenarios de comunicación V2I: alerta por V2I e intercambio de información por V2I. El escenario de alerta por V2I permite el intercambio de mensajes de alerta entre un vehículo y las infraestructuras. En el intercambio de información por V2I, un vehículo y la infraestructura se comunican entre sí para actualizar la información de tráfico y/o la información relativa a los servicios de información y entretenimiento. En el Cuadro 7-2 se muestran los datos de la comunicación V2I.

Cuadro 7-2 – Datos en la comunicación V2I

Categoría	Escenario	Datos
De vehículo a infraestructura	Alerta por V2I	• Mensaje de alerta
	Intercambio de información por V2I	• Señalización en el vehículo • Información en el vehículo • Fase de señal • Información sobre la temporización de los semáforos • Estado del asfalto • Condiciones meteorológicas • Condición de visibilidad • Información sobre obras en la vía pública

7.1.3 Datos en la comunicación V2D

En un escenario de comunicación V2D, el vehículo se comunica con dispositivos nómadas como un smartphone, un ordenador portátil y el sistema de navegación del vehículo. En [UIT-T X.1372] se identifican dos escenarios de comunicación V2D: comunicación V2D por enlaces indirectos y comunicación V2D por enlaces directos. La diferencia entre estos escenarios radica en la forma de comunicación, ya que en ambos se tratan los mismos tipos de datos. La comunicación V2P se considera un caso específico de la comunicación V2D en [UIT-T X.1372]. En el Cuadro 7-3 se muestran los datos de la comunicación V2D.

Cuadro 7-3 – Datos en la comunicación V2D

Categoría	Escenario	Datos
Dispositivo de vehículo a nómada	Comunicación V2D por enlaces indirectos/directos	• Datos del hardware del vehículo • Datos del software del vehículo • Datos del hardware del dispositivo • Datos del software del dispositivo • Datos de la plataforma de servicios • Datos de servicio de aplicación

7.2 Categorización de datos

En esta cláusula se describe la categorización de los datos que se tratan en la comunicación V2X.

Los datos de la comunicación V2X se tienen en cuenta para cumplir las leyes y disposiciones reglamentarias relacionadas con la protección de datos personales, como el Reglamento General de Protección de Datos (RGPD), y los datos descritos en la presente Recomendación no pueden referirse a la información de una persona concreta o identificable.

7.2.1 Datos de atributos de objeto

Los datos de atributos de objeto se refieren a los atributos de las entidades en la comunicación V2X, que pueden subdividirse en tres tipos, a saber: los atributos de los vehículos, los dispositivos móviles y las plataformas de servicios en la nube:

– Los atributos de los datos de los vehículos guardan relación con la propiedad de los vehículos, como la marca, el tipo, el logotipo y el color.

– Los atributos de los datos de un dispositivo móvil se refieren a la propiedad relacionada con dicho dispositivo, como la marca, el tipo y el color.

– Los atributos de los datos de la plataforma de servicios son las propiedades relacionadas con dicha plataforma, como la revisión, la fabricación y demás.

7.2.2 Datos de estado del vehículo

Los datos de estado del vehículo se refieren al estado de los vehículos, que está estrechamente relacionado con el servicio de información en la comunicación V2X. Incluyen los estados y parámetros de funcionamiento de esos sistemas, como el sistema de transmisión del automóvil, el sistema del bastidor, el sistema de seguridad del automóvil, el sistema de la carrocería, el sistema de confort del vehículo y el sistema eléctrico del automóvil.

Más concretamente, los datos de estado del vehículo incluyen información de datos del controlador del vehículo (como la señal de control de la bomba, la alarma del sensor de presión de aire, la señal de cableado del freno motor, etc.), el sistema de transmisión (como el par motor, la tasa de consumo de combustible, etc.), el sistema de refrigeración (como la temperatura del refrigerante), el sistema de la caja de cambios (como los datos de arranque y aceleración del vehículo, etc.), el sistema de seguridad (como el estado del airbag, el estado del uso del cinturón de seguridad, etc.), el sistema del bastidor (como los datos que reflejan el estado de la red del vehículo, el sistema de dirección, el frenado ABS, el control de la presión de los neumáticos, etc.), el sistema de confort (como los datos de la apertura del aire acondicionado, el ajuste del asiento, el sistema de ventanillas, el uso de la iluminación, etc.) y demás sistemas auxiliares.

Conforme a la descripción de los estados de funcionamiento del vehículo, los datos de estado de los vehículos pueden dividirse en dos tipos: datos de estado dinámicos de los vehículos y datos de estado estáticos de los vehículos.

– Los datos dinámicos de estado del vehículo están relacionados con los estados de funcionamiento de los sistemas del vehículo. Tomemos como ejemplo el estado del sistema de aire acondicionado, que depende de la temperatura y la humedad del coche.

– Los datos estáticos del estado del vehículo guardan relación con los estados estáticos de los sistemas de aire acondicionado, como el estado de uso del cinturón de seguridad y el estado del aire acondicionado, etc.

7.2.3 Datos de percepción del entorno

Los datos de percepción del entorno están relacionados principalmente con el entorno externo de los vehículos, como la información de datos de los equipos externos, los terminales, los peatones relacionados con la comunicación del vehículo o las interacciones de los servicios de información en la comunicación V2X, que incluye, entre otros datos, la velocidad, la información de los semáforos y la infraestructura vial en la comunicación de vehículo a vehículo. La información recopilada por los radares de control de la velocidad y por las cámaras asociadas a la infraestructura de la carretera, la dirección de la conducción y el movimiento, el estado de la conducción y el movimiento, la velocidad, la distancia, los posibles datos de estado relacionados con la colisión o la falta de incidencias, y los datos relacionados con las estaciones de carga y otros equipos adquiridos para los vehículos eléctricos también constituyen elementos de datos del entorno.

7.2.4 Datos de control del vehículo

Los datos de control del vehículo guardan relación con el control del vehículo en la comunicación V2X y se dividen en tres subtipos principales, a saber, los datos de control del vehículo para la conducción automática o el asistente de conducción inteligente, para el funcionamiento a distancia y para la conducción a distancia:

– Los datos de control del vehículo para la conducción automática o el asistente de conducción inteligente son los datos de las instrucciones de control relacionadas con la conducción automática o el asistente de conducción inteligente. Los datos se basan en el procesamiento de la percepción del entorno y los sistemas inteligentes de toma de decisiones y aportan información sobre el comportamiento del control inteligente de los vehículos, como el freno o la conducción por cable, el cambio automático de marchas y el control integrado del chasis.

– Los datos de control del vehículo para el funcionamiento a distancia se refieren a las instrucciones que reciben los vehículos a través de aplicaciones, plataformas de servicio, etc., como los datos de bloqueo/desbloqueo de puertas a distancia, control del aire acondicionado a distancia, accionamiento de ventanillas y luces a distancia, etc.

– En cuanto a los datos de control del vehículo para la conducción a distancia, cabe señalar que los casos de uso de la conducción a distancia se dividen a su vez en varios subcasos, en función de si el conductor a distancia es una persona o una "nube". Los datos de control del vehículo para la conducción a distancia abarcan las secuencias de imágenes de vídeo del exterior del vehículo que muestran la situación del carril alrededor del vehículo y las transmisiones de audio del exterior del vehículo enviadas al conductor a distancia para facilitarle la toma de decisiones. Por datos para la conducción a distancia se entienden también las transmisiones de vídeo o audio del interior del vehículo enviadas al conductor a distancia para el control de ciertas situaciones. Por otra parte, los datos de control del vehículo para la conducción a distancia se refieren asimismo a los datos relativos a las instrucciones de control a distancia enviadas por el conductor a distancia al vehículo para, por ejemplo, acelerar o maniobrar, que podrían generarse y transmitirse a raíz de un evento de control, como una instrucción de frenado [b-ETSI TR 126 985], [b-3GPP TR 22.886].

7.2.5 Datos de servicio de aplicación

Los datos de servicio de aplicación corresponden a la aplicación de la interacción de la información en la comunicación V2X. Se refieren a los datos relacionados con los servicios de información en la comunicación V2X, además de los datos de atributos de objeto, los datos de estado del vehículo, los datos de percepción del entorno, los datos de control del vehículo y los datos personales del usuario, incluidos, entre otros, los datos de información y entretenimiento, los datos de gestión y control de la seguridad del tráfico y los datos de servicios relacionados con el vehículo:

– Los datos de información y entretenimiento guardan relación con los servicios de entretenimiento prestados en las comunicaciones V2X, como la descarga multimedia, la navegación por páginas web y la suscripción a emisiones de una determinada población, así como la predicción meteorológica, etc.

– Los datos de gestión y control de la seguridad del tráfico están relacionados con la seguridad y la gestión del tráfico, como la alerta temprana de la seguridad del tráfico, el rescate de emergencia, la monitorización y la gestión de vehículos a distancia, etc.

– Los datos de servicios relacionados con el vehículo se refieren a los servicios posventa en la comunicación V2X, como el mantenimiento de vehículos, la gestión de vehículos de segunda mano, los seguros financieros y el comercio electrónico conexo. Por ejemplo, la frecuencia de mantenimiento de determinados tipos de piezas de automóviles de una determinada marca de automóviles forma parte de los datos de servicio relacionados con el vehículo.

7.2.6 Datos personales del usuario

Los datos personales del usuario se refieren a la información personal relativa al usuario, que se utiliza y/o genera en la comunicación V2X. En esta cláusula no se aborda la clasificación y protección de los datos personales de los usuarios.

Por lo tanto, si los datos enumerados en el Cuadro 7-4 a modo de ejemplo se corresponden con los datos personales del usuario amparados por la legislación relativa a la privacidad y por reglamentos como el RGPD, entonces la política de categorización queda anulada por ese reglamento.

7.3 Niveles de seguridad de los datos

Sobre la base de la consideración conjunta de los objetivos de seguridad de los datos, la importancia de los datos y el impacto de los posibles eventos de seguridad, cada categoría de datos puede clasificarse en 3 niveles:

– El **nivel 1** (datos menos protegidos) contiene datos disponibles públicamente en las comunicaciones V2X, como la versión del software de la plataforma V2X.

– El **nivel 2** (datos moderadamente protegidos) contiene datos que deben protegerse con medidas de seguridad, como los datos del vehículo obtenidos en la comunicación V2V, la cuenta de acceso y la contraseña de la comunicación V2X.

– El **nivel 3** (datos sumamente protegidos) contiene datos que deben estar más protegidos que el nivel 2 (datos moderadamente protegidos) en las comunicaciones V2X, como la información de las transacciones financieras en la comunicación V2D, los datos fundamentales de rendimiento del vehículo y la información de autenticación de identidad de las comunicaciones V2X.

Los datos confidenciales se refieren únicamente a los datos confidenciales de las empresas relacionados con la comunicación V2X, y no forma parte de ellos la información personal del usuario.

En el Cuadro 7-4 se ofrece información detallada sobre los niveles de seguridad de los datos, junto con ejemplos referidos a las comunicaciones V2X.

Cuadro7-4 – Ejemplos de niveles de seguridad de los datos en la comunicación V2X

Categoría de datos en las comunicaciones V2X		**Nivel de seguridad de los datos en las comunicaciones V2X**	**Ejemplos**
Datos de atributos de objeto	Datos de atributos del vehículo	Nivel 1	Marca, tipo, logotipo, color de un vehículo.
		Nivel 2	Parámetros de rendimiento de un determinado tipo de vehículo.
		Nivel 3	Datos de configuración de hardware y software específicos de un determinado tipo de vehículo.
	Datos de atributos del dispositivo móvil	Nivel 1	Marca, tipo, logotipo, color de un terminal móvil.
		Nivel 2	Datos del estado del equipo relacionados con algunas funciones importantes en la comunicación V2X.
		Nivel 3	Parámetros críticos de rendimiento e información de configuración de un tipo de dispositivo móvil.

Cuadro7-4 – Ejemplos de niveles de seguridad de los datos en la comunicación V2X

Categoría de datos en las comunicaciones V2X		**Nivel de seguridad de los datos en las comunicaciones V2X**	**Ejemplos**
	Datos de atributos de la plataforma de servicios en la nube	Nivel 1	Tipo y nombre de una plataforma de servicios en la nube.
		Nivel 2	Información del hardware, el sistema operativo o el software de las aplicaciones.
		Nivel 3	Parámetros críticos de rendimiento y la información de configuración de una plataforma de servicios.
Datos de estado del vehículo	Datos dinámicos del estado del vehículo	Nivel 1	Estado de un sistema de aire acondicionado. Temperatura interior de los vehículos.
		Nivel 2	Estado de funcionamiento de airbags y air belts, etc. Datos percibidos por los sensores del vehículo y estrechamente relacionados con aspectos importantes de la conducción, como la presión de los neumáticos.
		Nivel 3	Principales indicadores técnicos de funcionamiento del vehículo. Datos recibidos por los sensores del vehículo y estrechamente relacionados con aspectos críticos de la conducción, como los datos de los sensores de colisión.
	Datos estáticos del estado del vehículo	Nivel 1	Frecuencia de uso de un sistema de aire acondicionado en un momento determinado.
		Nivel 2	Consumo medio de combustible de un vehículo.
		Nivel 3	Datos confidenciales del sistema del vehículo.
Datos de percepción del entorno	Datos de percepción del entorno externo del vehículo	Nivel 1	Tipo de vía (autopista, carretera comarcal, acera), estado de la carretera (intacta, mojada, resbaladiza), límite de velocidad de la carretera, información sobre la distribución y el estado de las señales luminosas, información sobre el estado de las señales luminosas, congestión de la carretera, accidentes de tráfico, etc.
		Nivel 2	En el escenario de comunicación de vehículo a vehículo, información posterior a la desensibilización de los vehículos cercanos, como ubicación física, longitud y latitud, tiempo de actualización, velocidad de conducción, dirección de la marcha, información de cambio de carril. En el escenario de la comunicación de vehículo a peatón, los datos tras la desensibilización, como la ubicación, la distancia, la velocidad y el estado de movimiento de los peatones que se aproximan, y la posibilidad de colisión.

Cuadro7-4 – Ejemplos de niveles de seguridad de los datos en la comunicación V2X

Categoría de datos en las comunicaciones V2X		Nivel de seguridad de los datos en las comunicaciones V2X	Ejemplos
		Nivel 3	En los escenarios de comunicación de vehículo a vehículo, información de los datos de los vehículos adyacentes en un determinado periodo de tiempo después de la desensibilización, como trayecto, ubicación, hora, información de estacionamiento, etc.
Datos de control del vehículo	Datos de control del vehículo para la conducción automática o el asistente de conducción inteligente	Nivel 1	Datos fiables para los consejos de asistencia a la conducción.
		Nivel 2	En la aplicación de mantenimiento de carril del sistema inteligente de asistencia a la conducción, cuando el vehículo tiende a desviarse del carril de conducción, se envían los datos de comandos de advertencia, como la oscilación del volante o la indicación de luz roja o verde en el salpicadero.
		Nivel 3	Las instrucciones de confirmación del sistema de aparcamiento inteligente cuando se aparca de manera automática.
	Datos de control del vehículo para el funcionamiento a distancia	Nivel 1	Datos generales de lectura relacionados con el control de la comunicación V2X a distancia.
		Nivel 2	Instrucción para arrancar el vehículo a distancia o poner en marcha la conducción automática de los vehículos.
		Nivel 3	Implementación de instrucciones relacionadas con el control a distancia de múltiples vehículos, como una flota, a través de la plataforma de servicio de comunicaciones V2X.
	Datos de control del vehículo para la conducción a distancia	Nivel 1	El conductor a distancia podría utilizar las transmisiones de vídeo o audio del interior del vehículo, cuyos requisitos de retardo pueden ser menos estrictos que los de las transmisiones de vídeo y audio del exterior del vehículo, para supervisar el estado del interior del vehículo.
		Nivel 2	Las transmisiones de audio del exterior del vehículo podrían enviarse al conductor a distancia para hacerle partícipe de los ruidos y sonidos de claxon de otros vehículos.
		Nivel 3	Los sensores o dispositivos de reproducción, véanse pantallas o sistemas de sonido, se utilizan para transmitir las instrucciones de maniobra del conductor a distancia. Las instrucciones deben proporcionarse con niveles de fiabilidad elevada y latencia baja, y recibir acuse de recibo especialmente en relación con eventos de alarma (por ejemplo, instrucciones de frenado).

Cuadro7-4 – Ejemplos de niveles de seguridad de los datos en la comunicación V2X

Categoría de datos en las comunicaciones V2X		**Nivel de seguridad de los datos en las comunicaciones V2X**	**Ejemplos**
			Los datos de los sensores de vídeo (cámara) y audio (micrófono) (y quizás también de los sensores de radar o LIDAR) registran sonidos o vídeos externos para la identificación temprana y no visual de obstáculos en la carretera, como pueden ser vehículos de emergencia, peatones, etc. Los datos de los sensores de estado del vehículo (aceleración, velocidad, dirección, posición, etc.) podrían enviarse a intervalos fijos desde el vehículo al conductor a distancia con un nivel de fiabilidad elevado, ya que algunas transmisiones de sensores pueden ser esenciales para el correcto desarrollo de la conducción.
Datos de servicio de aplicación	Datos de información y entretenimiento	Nivel 1	Datos de emisión de radio.
		Nivel 2	Registros de navegación de compras en línea después de la desensibilización.
		Nivel 3	Grabaciones de voz y vídeo tras la desensibilización en aplicaciones de servicios de información.
	Datos de gestión y control de la seguridad del tráfico	Nivel 1	Alerta de congestión de tráfico, datos de alerta de accidentes de tráfico en tiempo real, etc.
		Nivel 2	Datos de alerta de colisión de vehículos por estacionamiento delante de un vehículo en cola.
		Nivel 3	Datos de seguimiento a distancia de vehículos de tráfico rodado.
	Datos de servicio relacionados con el vehículo	Nivel 1	Después de la desensibilización, se registran datos del comportamiento de uso del sistema de entretenimiento del vehículo relacionados con la utilización, el funcionamiento y otra información de dicho sistema.
		Nivel 2	Después de la desensibilización, datos de comportamiento del vehículo relacionados con la conducción del vehículo.
		Nivel 3	Datos posteriores a la desensibilización, como las preferencias personales del propietario del vehículo y los hábitos de comportamiento basados en la duración de los trayectos, la ruta, la ubicación y datos de comportamiento de uso del sistema de información y entretenimiento, o parámetros básicos del vehículo basados en los datos de percepción del estado y el entorno del propio vehículo, etc.
Datos personales del usuario	N/A	N/A	N/A

Cuadro7-4 – Ejemplos de niveles de seguridad de los datos en la comunicación V2X

Categoría de datos en las comunicaciones V2X	Nivel de seguridad de los datos en las comunicaciones V2X	Ejemplos
A continuación se describe el contenido del Cuadro 7-4: 1) N/A: no aplicable. 2) Los datos posteriores a la desensibilización descrita en el Cuadro 7-4 no pueden identificar o indicar directa o indirectamente la información personal de las personas, después de ser tratados por difusores anónimos y otros medios técnicos. Los métodos de desensibilización de datos incluyen, entre otros, el anonimato, la desidentificación, la diversidad, la supresión de datos, la alteración de datos, la privacidad diferencial, etc. La organización relacionada con la comunicación V2X debe tomar las medidas oportunas de desensibilización de datos basándose en la consideración integral de las características del interesado, el nivel de sensibilidad de los datos y los requisitos de funcionamiento de los datos.		

8 Requisitos de seguridad

En esta cláusula se presentan los requisitos de seguridad básicos, los requisitos de seguridad intermedios y los requisitos de seguridad avanzados que se corresponden estrictamente con los datos de nivel 1 a nivel 3.

8.1 Nivel de exigencia de seguridad

En función de la clasificación de los datos categorizados, se indican los métodos o medidas de seguridad para cada nivel. Existen tres niveles de requisitos de seguridad que pueden adoptarse: requisitos de seguridad básicos, requisitos de seguridad intermedios y requisitos de seguridad avanzados. En general, los requisitos de seguridad básicos se adoptan para proteger el nivel 1 (datos menos protegidos), los intermedios para proteger el nivel 2 (datos moderadamente protegidos) y los avanzados para proteger el nivel 3 (datos sumamente protegidos). En el Cuadro 8-1 se describen los requisitos de seguridad según el nivel de seguridad de los datos de comunicación V2X.

Las empresas también pueden elegir las medidas de seguridad en función de su propia situación o de la confidencialidad de los datos.

Cuadro 8-1 – Requisitos de seguridad según el nivel de seguridad de los datos de comunicación V2X

Nivel de seguridad de los datos de comunicación V2X	Nivel de requisitos de seguridad		
	Básico	Intermedio	Avanzado
Nivel 1 (datos menos protegidos)	*	N/A	N/A
Nivel 2 (datos moderadamente protegidos)	*	*	N/A
Nivel 3 (datos sumamente protegidos)	*	*	*
*: cubierto; N/A: no aplicable.			

8.2 Requisitos de seguridad básicos

1) Recopilación de datos

- Los datos en las comunicaciones V2X deben clasificarse según la combinación de los objetivos de seguridad de los datos, la importancia de estos últimos y el impacto de los posibles eventos de seguridad.
- En el proceso de recogida de datos se debe seguir el principio de minimización. Solo se pueden recopilar datos relacionados con las funciones empresariales.
- Los datos recogidos deben clasificarse y gestionarse de acuerdo con los métodos de clasificación de datos y clasificación descritos en las cláusulas 6 y 7. Deben formularse y aplicarse diferentes medidas de seguridad para los distintos niveles de datos.

2) Transmisión de datos

- El requisito de seguridad global de la transmisión de datos en las comunicaciones V2X no debería ser inferior al de la red de comunicación general.
- Según las diferentes categorizaciones de los datos, los procesos empresariales y los riesgos de seguridad de los escenarios de comunicación V2X, deben adoptarse diferentes estrategias y medidas de seguridad en la transmisión de datos.
- Los protocolos de seguridad, como la seguridad de la capa de transporte (TLS), deben utilizarse para garantizar la seguridad de la transmisión de datos en los escenarios de comunicación entre el vehículo y otras entidades.
- Deberían ser capaces de detectar que los datos se corrompieron durante la transmisión.

3) Almacenamiento de datos

- Respecto de los datos almacenados en los terminales de los vehículos y las plataformas de servicio, deben adoptarse mecanismos de cifrado de datos en los equipos y sistemas relacionados con la comunicación V2X. Los parámetros como el algoritmo, la fuerza y el procedimiento criptográfico deben ser soportados por una configuración opcional.
- Se debe garantizar la seguridad de los datos de la caché en la plataforma de servicios o el sistema del vehículo. Se deben cifrar los datos almacenados en el sistema de caché.
- En el caso de los datos almacenados en los terminales de vehículos y las plataformas de servicios, deben adoptarse mecanismos de control de acceso a los datos para evitar el acceso, la modificación y la eliminación no autorizados, así como el acceso a la información entre dominios.
- Se debe verificar la integridad de los datos en el proceso de almacenamiento para evitar la manipulación, supresión e inserción de datos. Se debe proporcionar información de advertencia al usuario cuando se destruya la integridad de los datos.

4) Uso de datos

- Los datos deben tratarse dentro del ámbito de la autorización, limitada a un mínimo conjunto de necesidades empresariales.
- El uso de los datos debe ser autorizado y verificado.
- La finalidad y el alcance de la utilización de los datos deben cumplir las prescripciones legislativas y reglamentarias nacionales pertinentes.
- Durante el análisis y la extracción de datos, los datos de origen y los resultados de la extracción deben estar firmados para evitar que los datos se borren de forma maliciosa, se manipulen o se abuse de ellos sin restricciones.
- Para la transferencia o exportación de datos entre dispositivos, sistemas y plataformas de la Internet de los vehículos, deben adoptarse medidas de gestión y técnicas que garanticen la seguridad.

5) Migración de datos

- Se debe evaluar la capacidad de seguridad antes de la migración de datos para garantizar la seguridad de ese proceso.
- La continuidad del negocio y de las aplicaciones debe estar garantizada cuando se migran datos entre diferentes dispositivos de datos.
- Se debe establecer un esquema de migración, evaluar su viabilidad y riesgos conexos y desarrollar, en consecuencia, las medidas de control de riesgos como preparación para la migración de datos.

6) Destrucción de datos

- Se debe establecer una estrategia de destrucción de datos y un sistema de gestión para aclarar el objeto y el proceso de destrucción. Se debe establecer el mecanismo de examen y aprobación de la destrucción de datos, y crear la función de supervisión correspondiente para supervisar el proceso de destrucción.
- Deben preverse medidas para borrar los datos que hayan alcanzado su límite de conservación, o, cuando los usuarios ya no den su consentimiento, los datos deben ser destruidos inmediatamente.
- Hay que tomar medidas para ayudar a limpiar los datos que quedan tras la migración de datos o los procesos empresariales.
- Deben preverse medidas para eliminar todas las copias de seguridad de los datos.

7) Copia de seguridad y restauración de datos

- Los mecanismos de copia de seguridad y recuperación de datos deben establecerse antes de la migración de datos.
- Se debe proporcionar una copia de seguridad y recuperación de datos local.
- Debe establecerse un mecanismo periódico de copia de seguridad de los datos completos, y el ciclo temporal recomendado no debería ser inferior a una vez por semana.
- Los datos de la copia de seguridad deben tener los mismos derechos de control de acceso y requisitos de almacenamiento seguro que los datos originales.

8.3 Requisitos de seguridad intermedios

Los requisitos de seguridad intermedios son un conjunto de superconjuntos de requisitos de seguridad básicos. A partir de los requisitos de seguridad básicos en cada fase del ciclo de vida de los datos, se añaden los siguientes requisitos:

1) Recopilación de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- Durante la recopilación de los datos de nivel 2, se debe hacer una copia de seguridad de los datos originales para evitar la omisión y la pérdida de datos.
- Deben adoptarse mecanismos de identificación para garantizar la autenticidad de la recopilación de datos.
- Deben adoptarse mecanismos de verificación de datos para garantizar la integridad de la recopilación de datos.

2) Transmisión de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- La transmisión de datos de la plataforma de servicios centrales del automóvil y de la Internet de los vehículos debe adoptar comunicación de red privada o una comunicación de red privada virtual para realizar el aislamiento de Internet.
- En la comunicación V2V/V2I, se debe contar con un certificado de identidad de confianza, capaz de verificar la identidad del nodo de transmisión de datos, y la información de autenticación no debería revelar información de privacidad.
- El vehículo debe ser capaz de identificar las solicitudes de conexión ilegales de las redes celulares para filtrar los paquetes maliciosos.
- En el caso de los datos de nivel 2, como los datos de las instrucciones de control remoto, debe verificarse la fiabilidad de la fuente de datos para garantizar que estos no sean falsos.

3) Almacenamiento de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- Se debe verificar la integridad de los datos en el proceso de almacenamiento para evitar la manipulación, supresión e inserción de datos, y se deben proporcionar las medidas de restauración necesarias cuando se destruya la integridad de los datos.
- La información de identificación debe establecerse para los archivos de datos almacenados en el vehículo inteligente conectado (ICV), las plataformas de servicio y las aplicaciones para evitar el uso de esos archivos en dispositivos y sistemas no autorizados.
- Respecto del sistema de caché de la plataforma de servicios en la comunicación V2X, deben mantenerse registros operativos específicos para proteger los datos de nivel 2 almacenados.
- Todo el proceso de gestión de registros de datos debe estar claramente establecido para prevenir las amenazas de repudio de datos.

4) Uso de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- En el caso de la consulta de datos de nivel 2, se deben realizar las operaciones de consulta, visualización externa, estadísticas y procesamiento difuso.
- El uso de los datos de nivel 2 debe ser auditado y se debe generar un registro de auditoría.

5) Migración de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- Hay que elaborar el plan de migración, evaluar su viabilidad y los riesgos conexos y, a continuación, formular las correspondientes medidas de control de riesgos para preparar la migración de datos.

6) Destrucción de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- Se debe asegurar que el espacio de almacenamiento de recursos relacionados con la comunicación V2X, como archivos, directorios y registros de bases de datos, no se libere ni se reasigne a otros usuarios hasta que estos recursos estén completamente vacíos.
- Por lo que se refiere al terminal de a bordo, con el fin de evitar la fuga de datos debido a la sustitución de los componentes del vehículo, se debe proporcionar la función de borrado de datos del terminal del vehículo, con el fin de garantizar que los datos borrados del terminal del vehículo no puedan recuperarse.

7) Copia de seguridad y restauración de datos

Además de cumplir con los requisitos básicos de seguridad, también deben cumplirse los siguientes requisitos:

- En el caso de los datos de las copias de seguridad locales o remotas, debe realizarse una copia de respaldo de los datos completos al menos una vez a la semana, complementada con copias de seguridad incrementales al menos una vez al día. Además, debe establecerse un mecanismo de respaldo múltiple.
- Los datos de las copias de seguridad deben ser almacenados y cifrados.

8.4 Requisitos de seguridad avanzados

Los requisitos de seguridad avanzados son un conjunto de superconjuntos de requisitos de seguridad intermedios. A partir de los requisitos de seguridad intermedios en cada fase del ciclo de vida de los datos, deben adoptarse todos los requisitos siguientes.

1) Recopilación de datos

- Los requisitos de protección son los mismos que los de los requisitos de seguridad intermedios.

2) Transmisión de datos

Además de cumplir los requisitos de seguridad intermedios, también deben cumplirse los siguientes requisitos:

- Se deben poder detectar daños en la integridad de los datos durante la transmisión y tomar las medidas necesarias para recuperar los datos cuando se detecten daños que afecten a la integridad.
- En el caso de los datos confidenciales de nivel L3, se debe adoptar la autenticación mutua para hacer frente a la amenaza de manipulación y fuga de datos causada por la suplantación de identidad de entidades externas.

3) Almacenamiento de datos

Además de cumplir los requisitos de seguridad intermedios, también deben cumplirse los siguientes requisitos:

- Se debe adoptar el esquema de almacenamiento de cifrado de seguridad con hardware para garantizar la confidencialidad de los datos confidenciales de los vehículos, las plataformas de servicio, las aplicaciones de terminales móviles inteligentes y la infraestructura vial.
- Se debe verificar la integridad de los datos en el proceso de almacenamiento para evitar la manipulación, supresión e inserción de datos, y se deben proporcionar las medidas de restauración necesarias cuando se destruya la integridad de los datos.

4) Uso de datos

Además de cumplir los requisitos de seguridad intermedios, también deben cumplirse los siguientes requisitos:

- La aprobación de la autoridad de operación secundaria debe llevarse a cabo mediante el modo de autorización multipersonal.

- Debe realizarse el aislamiento de la correlación de datos para evitar la fuga de datos debido al análisis de asociación de datos en diferentes sistemas, plataformas o aplicaciones.
- La desensibilización dinámica debe apoyarse en el uso de datos confidenciales.

5) Migración de datos

Los requisitos de protección son los mismos que los de los requisitos de seguridad intermedios.

6) Destrucción de datos

Además de cumplir los requisitos de seguridad intermedios, también deben cumplirse los siguientes requisitos:

- Se deben proporcionar medios para evitar la recuperación de los datos destruidos.

7) Copia de seguridad y restauración de datos

Además de cumplir los requisitos de seguridad intermedios, también deben cumplirse los siguientes requisitos:

- Deben preverse medidas de autenticación de seguridad, como la autenticación de identidad, para garantizar que las operaciones de copia de seguridad y recuperación de datos locales y remotas solo puedan realizarse con el conocimiento o el control de usuarios autorizados.

Bibliografía

[b-UIT-T X.1217] Recomendación UIT-T X.1217 (2021), *Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones.*

[b-UIT-T X.1751] Recomendación UIT-T X.1751 (2020), *Directrices de seguridad para la gestión del ciclo vital de macrodatos destinadas por los operadores de telecomunicaciones*.

[b-3GPP TR 22.886] 3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16).*

[b-ETSI TR 126 985] ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16).*

[b-ETSI TS 102 637-2] ETSI TS 102 637-2 (2011), *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*.

[b-SAE J2735] V2X Communications Message Set Dictionary, (julio de 2020).

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, 2023