UITPublicaciones
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de Normalización

Recomendación

UIT-T X.1380 (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)

Directrices de seguridad para sistemas de grabación de datos basados en la nube en entornos automovilísticos

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

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

Recomendación UIT-T X.1380

Directrices de seguridad para sistemas de grabación de datos de eventos basados en la nube en entornos automovilísticos

Resumen

Los grabadores de datos de eventos (EDR) son uno de los componentes más importantes instalados en vehículos que circulan por carretera para la grabación del estado del vehículo, sus movimientos y las actuaciones del usuario en caso de accidente. El análisis de los datos asociados a los eventos, puede permitir determinar la causa de un accidente y, en última instancia, utilizarlos para mejorar la seguridad en el entorno de la automoción. Un sistema de almacenamiento de datos para la conducción autónoma también es un componente importante para la grabación de datos reflejen con claridad las interacciones entre el conductor y el sistema de conducción autónoma. Sin embargo, los sistemas convencionales de grabación de datos de eventos graban y gestionan todos los datos de forma local y, por lo tanto, los datos pueden sufrir pérdidas y destrucción.

La computación en la nube se considera un elemento que permite el acceso a través de la red a un conjunto flexible y ampliable de recursos físicos o virtuales compartibles con facilidades para el autoaprovisionamiento y la administración de servicios a demanda. Industrias como la de la aviación ya están tratando de aplicar servicios basados en la nube para grabadores de datos de eventos con el objetivo de incrementar la seguridad en su entorno. Conforme a la tendencia actual en materia de conectividad entre vehículos, los EDR y los sistemas de almacenamiento de datos para la conducción autónoma se instalarán cada vez más a fin de aumentar su seguridad general. Sin embargo, los procesos de recopilación, transferencia, almacenamiento, gestión y uso de los datos grabados para las características específicas del entorno automovilístico presentan ciertas vulnerabilidades. Por lo tanto, es necesario estudiar las vulnerabilidades, los requisitos de seguridad y casos de uso de sistemas de grabación de datos basados en la nube en entornos automovilísticos.

La presente Recomendación UIT-T X.1380 proporciona directrices sobre la seguridad de los sistemas de grabación de datos basados en la nube en entornos automovilísticos. Se describen amenazas, vulnerabilidades, requisitos de seguridad y casos de uso de sistemas de grabación de datos en la nube en entornos automovilísticos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1380	03-03-2023	17	11.1002/1000/15106

Palabras clave

Amenazas a la seguridad, DSSAD, DSSAD basado en la nube, EDR, grabadores de datos, grabador de datos de eventos basado en la nube (EDR), nube, requisitos de seguridad.

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

Índice

Recomendación UIT-T X.1380

Directrices de seguridad para sistemas de grabación de datos de eventos basados en la nube en entornos automovilísticos

1 Alcance

La presente Recomendación proporciona directrices de seguridad para los sistemas de grabación de datos basados en la nube, tales como los grabadores de datos de eventos (EDR) y los sistemas de almacenamiento de datos para la conducción autónoma (DSSAD) en entornos de automoción. Esta Recomendación incluye consideraciones técnicas de los grabadores de datos, EDR y DSSAD. Además, este proyecto de Recomendación también incluye requisitos de seguridad y casos de uso.

2 Referencias

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

[UIT-T X.1371] Recomendación UIT-T X.1371(2020), *Amenazas a la seguridad de los vehículos conectados*.

3 Definiciones

3.1 Términos definidos en otros documentos

La presente Recomendación utiliza los términos siguientes definidos en otros documentos:

3.1.1 autentificación (*authentication*) [b-UIT-T X.1252]: Proceso formalizado de verificación que, si tiene éxito, permite que una entidad tenga una identidad autentificada.

3.1.2 sistema automatizado de mantenimiento de carril (*automated lane keeping system*) [b-UN R157]: Sistema que activa el conductor y que mantiene al vehículo dentro de su carril.

3.1.3 autorización (*authorization*) [b-ITU-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.4 disponibilidad (*availability*) [b-ITU-T X.800]: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.1.5 autenticidad (*authenticity*) [b-ITU-T X.641]: Protección para la autentificación mutua y la autenticación del origen de los datos.

3.1.6 imputabilidad (*accountability*) [b-ITU-T X.800]: Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.

3.1.7 confidencialidad (*confidentiality*) [b-ITU-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.8 sistema de almacenamiento de datos para la conducción autónoma (*data storage system for automated driving*) (DSSAD) [b-UN R157]: Sistema que permite determinar las interacciones entre los sistemas automatizado de mantenimiento de carril (ALKS) y el conductor humano.

3.1.9 grabadores de datos de eventos (*event data recorder*) (EDR) [b-UN R160]: Dispositivo o función de un vehículo que registra la dinámica del vehículo, datos de series temporales durante el periodo inmediatamente anterior a un evento (por ejemplo, velocidad del vehículo en el tiempo) o durante un evento accidente (por ejemplo, Delta V en el tiempo) destinados a ser recuperados después del evento colisión o accidente. Para los fines de esta definición, los datos de eventos no incluyen datos de audio o vídeo.

3.1.10 integridad de los datos (*data integrity*) [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.11 amenaza (*threat*) [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 interfaz en la nube (*cloud interface*): Pasarela del sistema en la nube que constituye la interfaz para las comunicaciones entre el sistema en la nube y los vehículos, usuarios o terceros.

3.2.2 sistema de gestión general (*general manager*): Componente de un sistema en la nube que rige los procedimientos básicos de almacenamiento y recuperación de información de grabadores de datos de eventos (EDR)/sistemas de almacenamiento de datos para la conducción autónoma (DSSAD) y que verifica los requisitos básicos de las peticiones de un usuario, un tercero o un vehículo.

3.2.3 servidor neutro (*neutral server*): Servidor independiente del fabricante del vehículo que puede proporcionar información anonimizada, información de identificación del vehículo (VII) o datos de grabadores de datos de eventos (EDR)/sistemas de almacenamiento de datos para la conducción autónoma (DSSAD) sin VII).

3.2.4 gestor de reglas y políticas (*rule/policy manager*): Componente de un sistema en la nube que actualiza las reglas y las políticas y que forma parte del sistema de gestión general.

3.2.5 coordinador de almacenamiento (*storage coordinator*): Componente de un sistema en la nube que separa datos de los grabadores de datos de eventos (EDR)/sistemas de almacenamiento de datos para la conducción autónoma (DSSAD)e información de identificación del vehículo (VII) para almacenar y recuperar los datos del almacenamiento en la nube mediante una política predeterminada.

4 Abreviaturas y acrónimos

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

ALKS	Sistema automatizado de mantenimiento de carril (*automated lane keeping systems*)
API	Interfaz de programación de aplicaciones (*application programming interface*)
CAN	Red de área del controlador (*controller area network*)
DoS	Denegación de servicio (*denial of service*)
DSSAD	Sistema de almacenamiento de datos para la conducción autónoma (*data storage system for automated driving*)
ECU	Unidad de control electrónica (*electronic control unit*)
EDR	Grabador de datos de eventos (*event data recorder*)
FIFO	Primero en entrar, primero en salir (*first-in-first-out*)
IVN	Red intravehicular (*in-vehicle network)*
JTAG	Grupo de acción de prueba conjunta (*joint test action group*)

MAC	Código de autentificación de mensajes (*message authentication code*)
MRM	Maniobra de riesgo mínimo (*minimum risk manoeuvre*)
OBD	Diagnóstico a bordo (*on-board diagnostic*)
OTA	Por vía aérea (*over-the-air*)
PII	Información de identificación personal (*personally identifiable information*)
RGPD	Reglamento General de Protección de Datos (*general data protection regulation*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
UDS	Servicios de diagnóstico unificado (*unified diagnostic services*)
V2X	Vehículo con su entorno (*vehicle-to-everything*)
VII	Información de identificación del vehículo (*vehicle identifiable information*)
VIN	Número de identificación del vehículo (*vehicle identification number*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

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

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para declarar la conformidad.

6 Sistemas de grabación de datos basados en la nube

6.1 Sistema de grabación de datos de eventos basado en la nube

Un EDR basado en la nube es un EDR conectado a sistemas en la nube (servidor soporte) para mejorar la accesibilidad y seguridad de los datos EDR en entornos de vehículos conectados y autónomos.

Un EDR es un dispositivo que hoy en día se instala en la mayoría de los automóviles para grabar información relacionada con colisiones o accidentes del vehículo a fin de mejorar la seguridad y la calidad de vida en el entorno del vehículo.

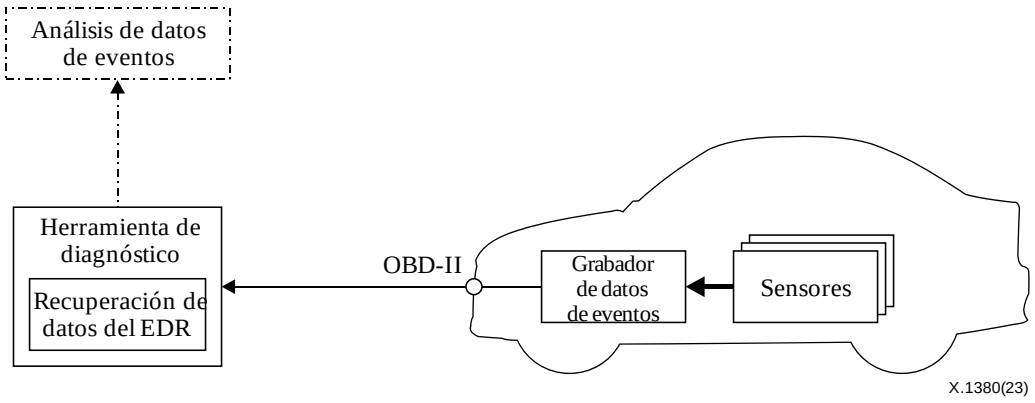

Figura 1 – EDR convencional para la automoción

Tal como se muestra en la Figura 1, el EDR convencional se activa cuando se produce un evento en el que se dan determinadas condiciones relativas al estado del vehículo, como el despliegue del airbag frontal, la superación del umbral de aceleración/desaceleración, el vuelco, etc. Cuando se activa el EDR, éste recoge un conjunto de datos predeterminado de los sensores y, a continuación, almacena los datos en su sistema de almacenamiento interno en memoria no volátil. En la práctica, los datos se graban desde –5 segundos antes del instante en que se produce el suceso desencadenante (normalmente denominado T0) hasta +500 milisegundos después del mismo. "–5 segundos" y "+500 milisegundos" y varían en función de la reglamentación nacional o de los fabricantes de vehículos.

Por lo general, el EDR tiene capacidad para almacenar en el vehículo más de un evento. Cuando el almacenamiento se colma con datos de eventos anteriores, los nuevos datos se escriben sobre los datos más antiguos. En eventos especiales como la apertura del airbag, el EDR convencional almacena los datos recopilados y bloquea el almacenamiento de datos para evitar que sean manipulados o sobrescritos.

Los datos almacenados se recuperan a través del puerto de diagnóstico a bordo (OBD)-II utilizando la herramienta de diagnóstico o de recuperación designada y se emplean para analizar la colisión o el accidente. El conjunto mínimo de datos recogidos viene determinado por la reglamentación nacional sobre vehículos o por el diseño del fabricante del vehículo. Además, el formato de los datos de eventos grabados suele diferir en función del fabricante del vehículo y a menudo difieren según el modelo del vehículo. Por lo tanto, a la hora de recuperar y analizar datos de eventos, se requiere utilizar un software de recuperación especializado.

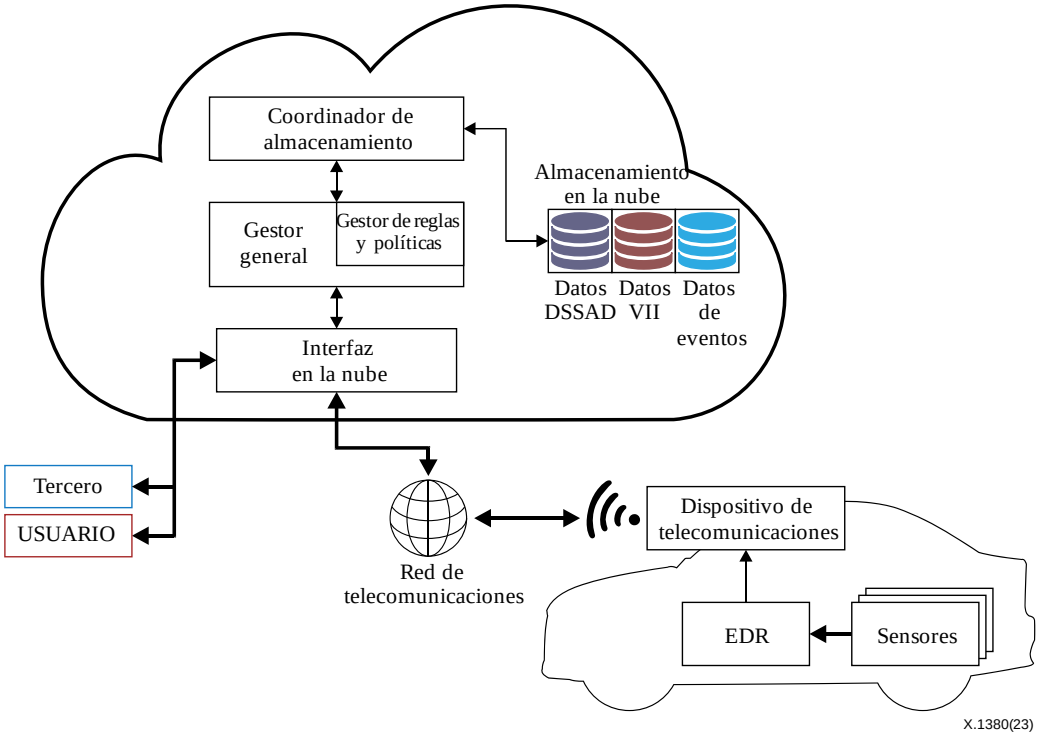

Figura 2 – EDR basado en la nube

Un EDR basado en la nube, descrito en la Figura 2, almacena datos de eventos en los sistemas en la nube a través de un dispositivo de telecomunicación conectado al EDR.

El conjunto de datos de la grabación puede ser diferente de los conjuntos de datos EDR convencionales debido a las diferencias sistemáticas y ambientales entre los EDR convencionales y los EDR basados en la nube. Asimismo, podría añadirse un nuevo tipo de datos procedentes de la

unidad de control electrónico (ECU) que rige la conducción autónoma, ya que son los datos críticos que ayudan a analizar los accidentes de los vehículos autónomos.

A diferencia del EDR convencional, que sobrescribe los nuevos datos de eventos sobre los datos de eventos desbloqueados, el EDR basado en la nube puede grabar los datos de eventos en el almacenamiento en la nube sin sobrescribir datos. Así, el EDR basado en la nube puede tener todos los datos grabados de un vehículo sin borrar ninguno. Esta es una de las mayores ventajas del EDR basado en la nube, ya que facilita enormemente la investigación de la seguridad vial utilizando los datos completos del EDR.

Los datos EDR recogidos y almacenados en los servicios en la nube deben estar a disposición de los usuarios o de terceros si alguna parte solicita acceso a los mismos en el marco del debido proceso y con la autorización pertinente. Al entregar a las partes los datos EDR solicitados, debe aplicarse un proceso de autenticación para verificar la validez de la solicitud.

Además de las funciones de almacenamiento y suministro de datos EDR, el EDR basado en la nube también proporciona actualizaciones de reglas y políticas del sistema. Cualquier usuario o tercero puede solicitar la actualización de reglas y políticas para el dispositivo EDR del vehículo y la política correspondiente en el sistema en la nube. La solicitud requeriría una autoridad y verificación de seguridad de mayor nivel que cualquier procedimiento ordinario de almacenamiento y recuperación.

En el sistema EDR basado en la nube de la Figura 2, las entidades de los sistemas en la nube están definidas para funcionar a un nivel superior que las funcionalidades del EDR basado en la nube. La interfaz en la nube es una pasarela del sistema en la nube y mantiene el registro de los accesos autorizados. El gestor general gobierna los procedimientos básicos de almacenamiento y recuperación de datos EDR. Verifica los requisitos básicos de la solicitud del usuario, de una tercera parte o del vehículo, y también ejecuta las actualizaciones de las reglas y políticas con la ayuda de los gestores integrados de reglas y políticas. El coordinador de almacenamiento almacena y recupera los datos de eventos basándose en una política predeterminada. La política puede incluir el cribado de los datos EDR recuperados del almacenamiento en la nube en virtud de la autoridad del solicitante. También puede incluir la metodología de almacenamiento y recuperación de datos EDR en el almacenamiento en la nube.

6.2 Sistema de almacenamiento de datos basado en la nube para la conducción autónoma

El sistema de almacenamiento de datos para la conducción autónoma (DSSAD) es un sistema que pretende arrojar luz sobre quién solicitó conducir y quién conducía (algo que puede ser diferente, especialmente durante los procedimientos de transición) mediante el almacenamiento de un conjunto de datos que proporciona una imagen clara de las interacciones entre el conductor y el sistema de conducción autónoma. El DSSAD ha sido reconocido en [b-UN R157]. El reglamento reconoce el DSSAD como un requisito para vehículos de conducción autónoma.

El DSSAD almacena información como la activación del sistema de conducción autónoma, la desactivación, las maniobras de emergencia en las demandas de transición, etc. Cuando se desactiva el estado del sistema automatizado o se demanda una transición, el motivo del cambio de estado se almacena en el DSSAD. Las partes interesadas pueden aclarar quién solicitó la conducción y quién realizó la conducción real analizando los datos del DSSAD que graba la interacción entre el sistema automatizado y el conductor.

El DSSAD basado en la nube, descrito en la Figura 3, almacena los datos DSSAD en los sistemas en la nube a través de un dispositivo de comunicación conectado al DSSAD. El proceso por el que los datos DSSAD se envían al sistema en la nube es el mismo que el del EDR basado en la nube. La diferencia es que los datos DSSAD se envían en lugar de los datos EDR. El DSSAD transmite periódicamente los datos DSSAD al sistema en la nube. Así, los DSSAD pueden responder con flexibilidad a problemas debidos a sus propias limitaciones del almacenamiento.

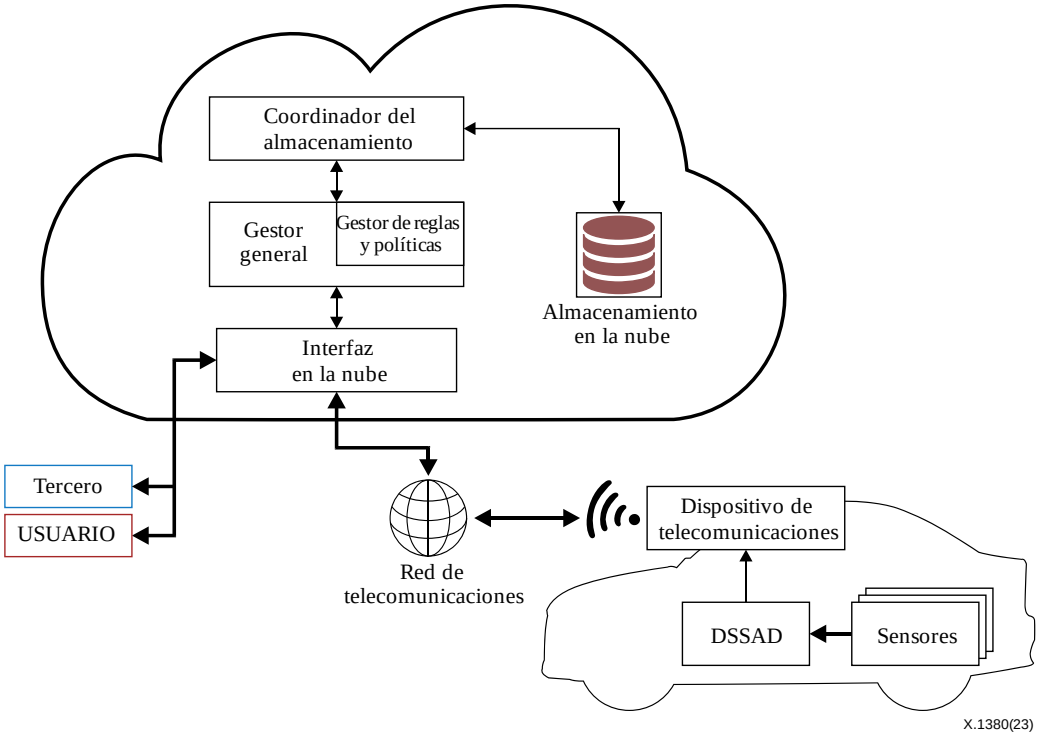

Figura 3 – DSSAD basado en la nube

6.3 Comparación entre EDR y DSSAD

En el Cuadro 1 se muestra una comparativa entre el EDR y el DSSAD.

Cuadro 1 – Comparación entre el EDR y el DSSAD

	EDR	DSSAD
Propósito	Análisis y reconstrucción de accidentes	Clarifica la responsabilidad del vehículo en momentos específicos; quién solicitó conducir y quien conducía
Condición desencadenante	Evento (por ejemplo, una colisión): ocurrencia física que hace que se supere el umbral desencadenante	Interacción: modifica el estado de funcionamiento del sistema, o solicita una modificación del mismo
Datos recopilados	Conjunto de datos predeterminados pertinentes para el análisis de una colisión	Conjunto de datos predeterminados pertinentes relativos al control del vehículo y la responsabilidad
Tiempo de almacenamiento	Datos grabados cuando se desencadena el proceso (momentáneos)	Datos grabados durante toda la conducción
Hora de la carga de datos	Todo momento de almacenamiento, arranque y parada	

7 Diseño de un sistema de grabación de datos basado en la nube

7.1 Gestión de los datos EDR

El propósito del EDR es almacenar información del vehículo relacionada con eventos específicos, como la apertura de un airbag. Los datos grabados en el EDR se utilizan para el análisis y la reconstrucción de accidentes. Por lo tanto, el EDR graba la hora de un evento y el estado del vehículo en el momento en que se produjo el evento.

7.1.1 Hora de grabación de los datos de un evento

La Figura 4 describe cómo el EDR graba un evento. Cuando el EDR detecta un evento específico, establece la hora del evento como T0 del evento que ha tenido lugar, y a continuación recopila los datos designados en un periodo de grabación predeterminado, que tiene una duración predefinida. T_0^n denota la hora de ocurrencia del *n-ésimo* evento. El marco temporal de la grabación puede diferir según los tipos de eventos, ya que cada tipo de evento tiene distintas condiciones desencadenantes. T_{pre} denota el tiempo anterior a un evento específico. T_{post} denotes el tiempo posterior al evento. El marco temporal puede describirse como $[(T_0 - T_{pre}) \sim (T_0 + T_{post})]$.

En el caso de que se produzcan varios eventos consecutivos, como se describe en la Figura 4, el EDR graba los datos con independencia de que los sucesivos periodos se solapen. La Figura 4 a) muestra tiempos de grabación de eventos no solapados. La Figura 4 b) muestra los tiempos de grabación de eventos solapados.

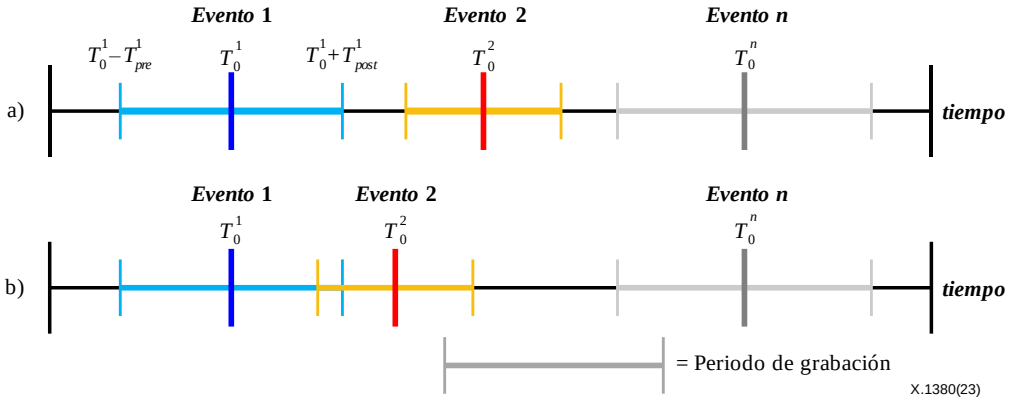

Figura 4 – Periodos de grabación del EDR:
a) eventos no solapados; b) eventos solapados

7.1.2 Bloqueo de los datos almacenados en un vehículo

Existen varios dispositivos de almacenamiento en vehículos para los datos EDR. Dada la diversidad de las condiciones predeterminadas, pueden producirse múltiples eventos consecutivos. El proceso de almacenamiento del EDR sigue el procedimiento FIFO (primero en entrar, primero en salir). Si todos los dispositivos de almacenamiento de EDR están llenos por eventos anteriores, los nuevos datos de eventos sobrescriben los más antiguos. Sin embargo, algunas condiciones predeterminadas desencadenantes de eventos, como el despliegue del airbag frontal, requieren el bloqueo del almacenamiento de datos después de la escritura de los datos para evitar la sobreescritura sobre datos almacenados. La Figura 5 muestra un ejemplo de procedimientos de grabación del EDR con dos unidades de almacenamiento. La Figura 5 a) muestra el proceso de almacenamiento de datos para los eventos subsiguientes sin bloqueo de datos, mostrando que el evento 3 se sobrescribe en el dispositivo de almacenamiento que contiene los datos de eventos anteriores. Por otro lado, b) y c) muestran el proceso de almacenamiento de datos de eventos posteriores con bloqueo de datos, que muestran que el evento siguiente no se puede sobrescribir sobre la información almacenada con bloqueo de datos. Específicamente, en el proceso c), el evento 3 no puede almacenarse en ningún dispositivo de almacenamiento porque ambos están llenos y bloqueados con datos de eventos anteriores, a saber, el evento 1 y el evento 2. Por lo tanto, se deberá establecer una política que establezca la prioridad con la que se deben bloquear los datos en los dispositivos de almacenamiento.

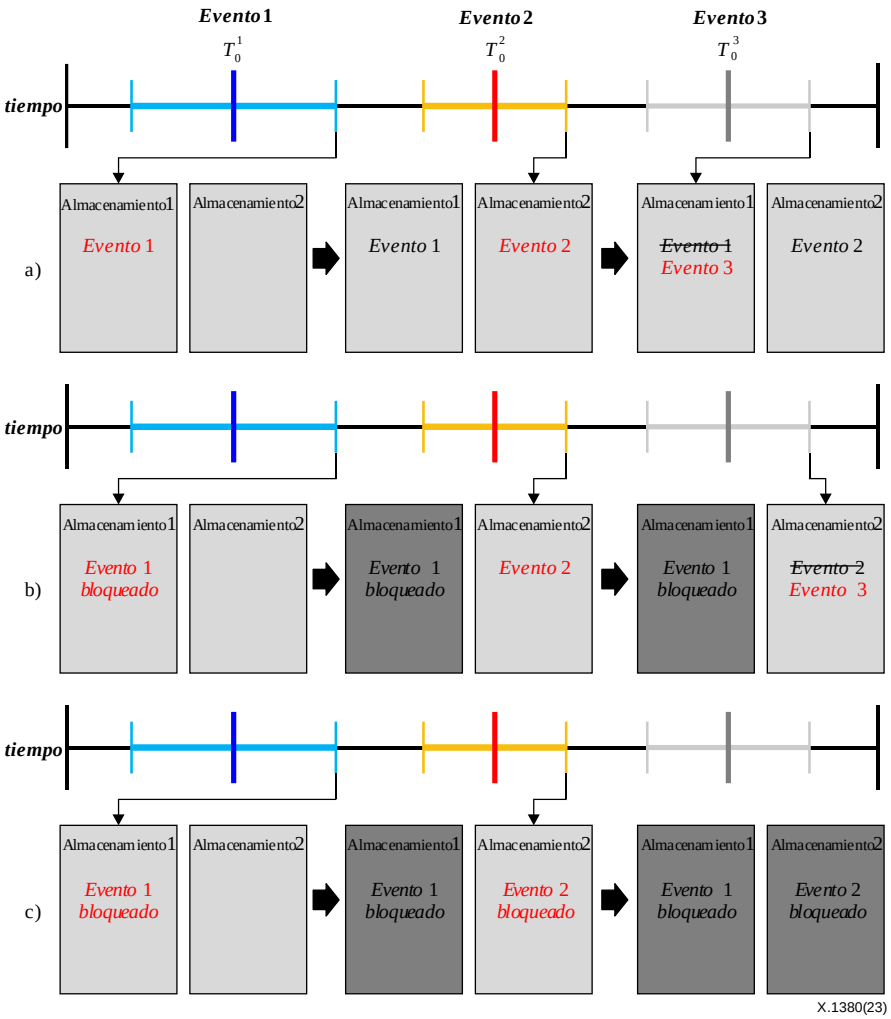

Figura 5 – Ejemplo de EDR con dos dispositivos de almacenamiento: a) sin bloqueo de datos, b) con bloqueo de datos sólo del evento 1, c) con bloqueo de datos del evento 1 y del evento 2

7.1.3 Ampliación del conjunto de datos

Por lo general, las administraciones nacionales o los fabricantes de vehículos han normalizado el conjunto de datos EDR convencionales. Es necesario ampliar el conjunto convencional de datos EDR para los vehículos conectados y autónomos. Por ejemplo, los datos de sensores como el radar y el lidar utilizados en el vehículo de conducción autónoma pueden ser fundamentales para investigar los accidentes. Además, los certificados almacenados utilizados en la comunicación entre el vehículo y su entorno (V2X) durante un evento pueden ser esenciales para el conocer el entorno del vehículo conectado. Además, los registros almacenados en un sistema de detección de intrusos (IDS) en relación con anomalías y firmas de intrusión son cruciales para aclarar si el evento se ha debido a un ciberataque.

7.2 Gestión de los datos DSSAD

7.2.1 Tiempo de grabación del DSSAD

La Figura 6 muestra la diferencia en términos de tiempo de grabación de datos entre el EDR y el DSSAD. El DSSAD graba todas las interacciones predefinidas entre el sistema automatizado y el conductor, mientras que el EDR graba durante un tiempo predeterminado cada vez que ocurren eventos desencadenantes. Por lo tanto, los datos grabados en el EDR y el DSSAD son útiles para determinar quién tenía el control del vehículo en el momento del accidente.

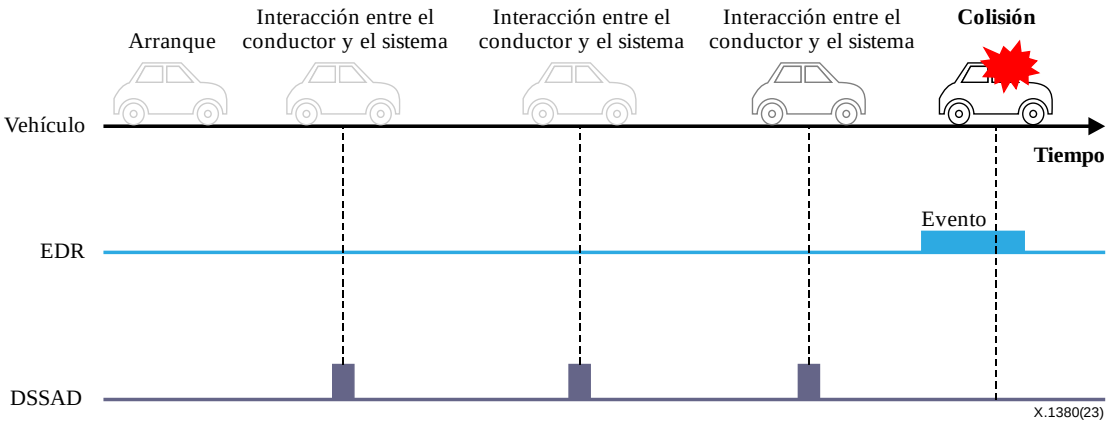

Figura 6 – Tiempo de grabación de datos del EDR y del DSSAD

El DSSAD basado en la nube debe transmitir los datos al sistema en la nube conforme a una política predefinida. Cuando la capacidad de almacenamiento del DSSAD en el vehículo alcanza su límite, los datos más recientes pueden sobrescribir los datos anteriores de acuerdo con el procedimiento FIFO.

7.2.2 Bloqueo de datos almacenados en un vehículo

El proceso de almacenamiento del DSSAD también sigue el procedimiento de primero en entrar, primero en salir (FIFO), al igual que el proceso de almacenamiento del EDR. Si el dispositivo de almacenamiento del DSSAD está lleno, los datos sobrescriben los más antiguos. Sin embargo, la condición predeterminada para desencadenar eventos con bloqueo de datos en el almacenamiento del EDR requiere el bloqueo del almacenamiento de datos DSSAD tras la escritura de los datos, al tiempo que se rechazan las sobreescrituras que puedan afectar a datos almacenados. El formato de los datos DSSAD bloqueados viene determinado por la política de almacenamiento de datos DSSAD. El formato de los datos DSSAD bloqueados puede diferir del formato de datos DSSAD estándar.

Tras el bloqueo de los datos DSSAD, los datos bloqueados pueden transmitirse al sistema en la nube. La transmisión de los datos DSSAD bloqueados puede ser prioritaria con respecto a otras transmisiones de datos, como los datos DSSAD normales y los datos EDR bloqueados. Si se confirma la compleción de la transmisión, los datos transmitidos pueden eliminarse del dispositivo de almacenamiento DSSAD en el vehículo.

7.2.3 Formato de los datos

Mientras que la finalidad del EDR es grabar los datos de un evento, el objetivo del DSSAD es identificar quién tiene la responsabilidad en un momento dado (normalmente el momento del accidente).

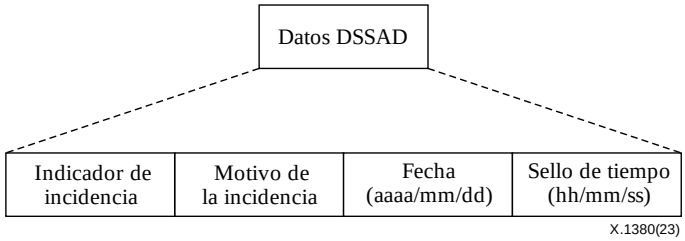

Figura 7 – Formato de los datos del DSSAD

Tal como se muestra en la Figura 7, los datos DSSAD constan de cuatro campos (véase [b-UN R157]).

El "indicador de incidencia" es un campo que indica el tipo de interacción entre el conductor y el sistema, tales como las demandas de transición y las maniobras de emergencia.

El campo "motivo de la incidencia" indica por qué se activó la indicación de incidencia. Este campo contiene la motivación detallada de la transición. En la cláusula 8.2 de la [b-UN R157] figuran los motivos que dan lugar a las incidencias.

El campo "fecha" es la fecha en que se crea el indicador de incidencia. Los datos de este campo tienen la forma de año/mes/día.

El campo "sello de tiempo" es la hora en la que se genera el indicador de incidencia. Los datos de este campo tienen la forma de "hora/minuto/segundo, zona horaria". Debido a las características del DSSAD, se requiere disponer de un sello de tiempo con una elevada precisión. Se puede admitir un mismo sello de tiempo para múltiples datos DSSAD grabados simultáneamente dentro de la resolución temporal de un determinado dato del DSSAD. Si se producen varios eventos en un segundo, los eventos pueden tener el mismo sello de tiempo. En este caso, los datos DSSAD deben indicar el orden temporal.

7.3 Información de identificación del vehículo (VII)

Cuando el EDR o el DSSAD carga sus datos en los sistemas en la nube, se debe tener en cuenta la VII para identificar los datos. La VII puede ser el número de la matrícula del vehículo, el certificado del vehículo, el número de identificación del vehículo (VIN) o cualquier dato que pueda utilizarse para la identificación del vehículo. La VII puede considerarse información de identificación personal (PII).

En lo que respecta a los futuros entornos automovilísticos, hay que tener en cuenta las situaciones en las que varios usuarios comparten un mismo vehículo, como es el caso en el concepto comercial de vehículo compartido. Cuando un usuario desee utilizar sistemas EDR/DSSAD basados en la nube mientras conduce, el vehículo compartido debería ser capaz de distinguir al usuario conductor. Sin embargo, es difícil identificar a cada usuario porque no existe un proceso obligatorio para que el vehículo recopile información de un usuario (por ejemplo, su ID). La información del usuario podría obtenerse mediante sistemas personalizados, como la clave digital del smartphone, que utiliza un proceso de autenticación mediante el certificado único del usuario. De este modo, se podría recopilar y enviar la información del usuario como parte de la VII.

Como se describe en la cláusula 6.1, los datos EDR se recopilan cuando en un vehículo se producen eventos desencadenantes predeterminados, mientras que los datos del DSSAD se recopilan siempre que hay una interacción entre vehículo y conductor. Dado que el EDR y el DSSAD están vinculados a un vehículo y que los datos se recopilan para cada vehículo, la identificación del vehículo es una tarea fundamental del sistema EDR/DSSAD basado en la nube. Por lo tanto, el VII se compone de los siguientes elementos:

– **Información del vehículo** (obligatoria): datos de identificación de un vehículo en particular, por ejemplo, el VIN.

– **Información del usuario** (facultativa): datos de identificación de un usuario o conductor.

La Figura 8 muestra el proceso de transmisión del EDR/DSSAD desde el vehículo a la nube.

El EDR/DSSAD recopila los datos de cada sensor y la unidad de control electrónica (ECU) en la red intravehicular de acuerdo con las reglas predefinidas y luego los transmite al dispositivo de telecomunicaciones. El dispositivo de telecomunicación añade la VII a los datos que recopila el EDR/DSSAD y la envía al sistema en la nube. Los datos EDR/DSSAD y la VII recibidos a través de la interfaz en la nube se transfieren al gestor de almacenamiento y posteriormente se almacenan de acuerdo con la política del sistema en la nube.

Solamente usuarios autorizados pueden acceder a los datos EDR/DSSAD almacenados en la nube. Por lo tanto, los usuarios que deseen obtener información del sistema en la nube deben transmitir información de autenticación que demuestre su identidad. El sistema en la nube proporciona los datos EDR/DSSAD a los usuarios autentificados.

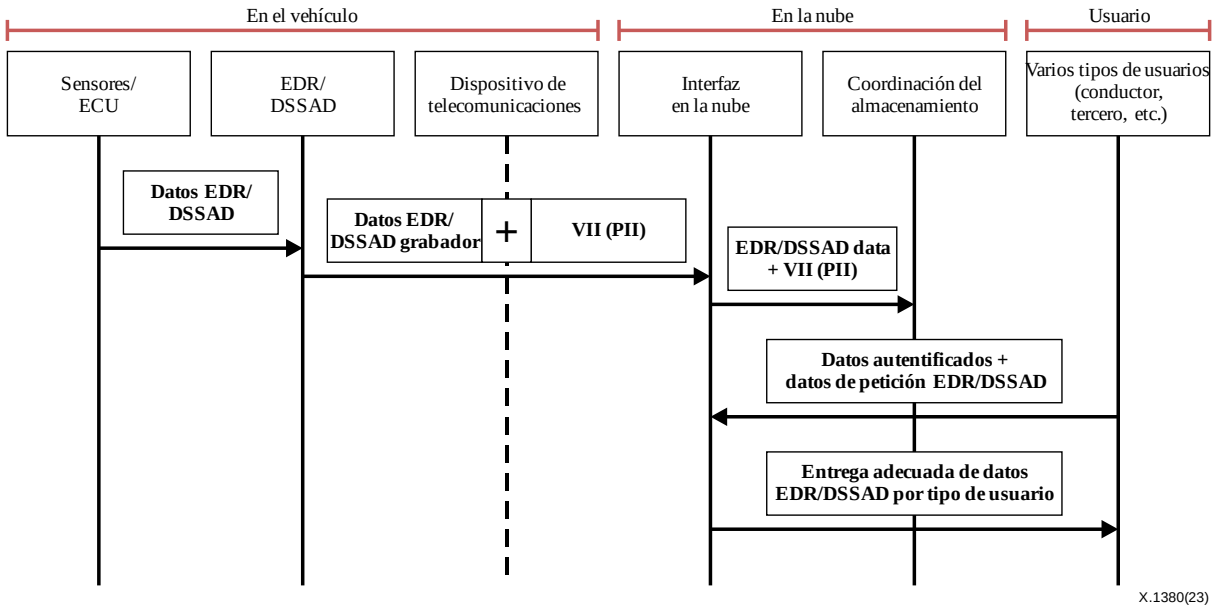

Figura 8 – Flujo de datos del EDR/DSSAD basado en la nube

7.4 Sistemas en la nube para EDR y DSSAD

7.4.1 Aumento de la accesibilidad a los datos grabados

El EDR convencional tiene un punto de acceso en el puerto OBD-II. Sólo a través del puerto OBD-II y de la herramienta de diagnóstico del vehículo se pueden recuperar y utilizar los datos EDR. Esta es la razón por la que los datos EDR rara vez son utilizados por los propietarios de los vehículos, a pesar de que son los dueños de los datos.

Por otro lado, los EDR/DSSAD basados en la nube ofrecen a los usuarios una mayor accesibilidad a los datos EDR/DSSAD mediante la carga de esos datos en entornos en la nube. Los usuarios o terceros pueden utilizar sus identificaciones VII o predeterminadas para cargar sus datos EDR/DSSAD para un uso posterior. Esto puede permitir una ampliación escalable de los datos EDR/DSSAD y contribuir a mejorar la seguridad vial.

7.4.2 Actualización de reglas y políticas

Un sistema EDR/DSSAD basado en la nube ofrece la función de actualización de reglas y políticas. Una regla define cómo manejar los datos en un vehículo y una política define cómo gestionar los datos en la nube. La regla consta de la condición del evento, el tipo de datos grabados, el tiempo de grabación de un determinado tipo de datos y el procedimiento de carga de datos del vehículo. La política aplicable en el contexto de EDR/DSSAD basado en la nube, incluye el permiso de acceso a los datos que se concede a las partes. En los sistemas en la nube la política es gestionada por un coordinador de almacenamiento que archiva los datos EDR/DSSAD.

Los sistemas EDR/DSSAD basados en la nube ofrecen una función de actualización de reglas y políticas. En general, los responsables de la reglamentación nacional definen el conjunto de datos de los eventos obligatorios y sus condiciones. Con arreglo a las actualizaciones de la reglamentación por parte de las autoridades competentes y mediante una solicitud legítima realizada por el usuario o por un tercero, el sistema EDR/DSSAD basado en la nube ejecuta las actualizaciones de las reglas y políticas en el vehículo y en la nube.

8 Análisis de las amenazas a la seguridad

8.1 Activos de la seguridad y objetivos de seguridad conexos

Un activo de seguridad es cualquier objeto, función o recurso de datos que debe ser protegido. En el Cuadro 2 y a partir de un análisis de los sistemas EDR/DSSAD basados en la nube se muestran diversos activos y objetivos de seguridad conexos.

Cuadro 2 – Activos de seguridad y objetivos de seguridad conexos

Activo de seguridad	Descripción	Objetivos de seguridad conexos
Datos EDR/DSSAD almacenados en un vehículo	Datos EDR/DSSAD recopilados en el vehículo	Integridad
Reglas EDR/DSSAD almacenadas en un vehículo	Reglas del EDR/DSSAD que pueden ser actualizadas por la política en la nube	Integridad
Firmware EDR/DSSAD	Firmware del dispositivo EDR/DSSAD	Integridad
Paquete de transmisión aérea (OTA)	Paquete OTA utilizado para actualizar las reglas EDR/DSSAD	Confidencialidad, integridad
Tráfico de bus	Tráfico de bus transmitido en una red intravehicular	Confidencialidad, integridad
Registro de EDR/DSSAD	Auditoría de registros de dispositivos EDR/DSSAD	Integridad, responsabilidad
Comunicación con los sistemas de depuración y diagnóstico	Comunicación entre el dispositivo EDR/DSSAD y las herramientas de depuración o de diagnóstico	Confidencialidad, autenticidad
Comunicación con el sistema soporte	Comunicación entre el sistema soporte y los vehículos o usuarios/terceros	Confidencialidad, autenticidad, disponibilidad
Política en la nube	Política en la nube	Integridad
VII	Datos privados usados para identificar usuarios/vehículos	Confidencialidad
Registro en la nube	Auditoría de registros para políticas en la nube, peticiones de usuarios/terceros y otros comportamientos que puedan afectar a la seguridad en la nube	Integridad, responsabilidad
Datos de EDR/DSSAD almacenados en la nube	Datos EDR/DSSAD recibidos de vehículos	Integridad

8.2 Amenazas a la seguridad

Esta cláusula describe amenazas a la seguridad en los sistemas de grabación de datos basados en la nube. Las amenazas generales identificadas en los vehículos conectados se describen en [ITU-T X.1371].

8.2.1 Amenazas a la confidencialidad

Los datos incorporados a los sistemas de grabación de datos basados en la nube son generalmente datos privados de los usuarios. La propiedad y el alcance de la recopilación de datos pueden variar según la reglamentación que rija para el vehículo en cuestión; sin embargo, los datos del sistema de grabación se consideran por lo general información de identificación del vehículo (VII). La incapacidad de mantener la confidencialidad de los datos en los sistemas de grabación de datos en la nube puede considerarse una invasión a la privacidad de los datos de los usuarios. Por ejemplo, la escucha clandestina y la interceptación pueden ser amenazas típicas a la confidencialidad.

– **Escucha clandestina**: En redes inalámbricas, como las que soportan los servicios en la nube, una escucha del medio de comunicación es un potencial ataque de fácil ejecución. Existen dos maneras en que un atacante puede inspeccionar ilegalmente los mensajes, incluido el VII de los sistemas de grabación de datos en la nube. En primer lugar, puede hacerlo entre el vehículo y el servidor en la nube. En este caso, pueden filtrarse los datos de eventos de los vehículos y los datos de actualización de reglas y políticas de un servidor en la nube.

  En segundo lugar, puede producirse un ataque entre el usuario o un tercero y los sistemas en la nube. En este caso, pueden filtrarse datos de eventos del sistema en la nube y las solicitudes de actualización de reglas y políticas realizadas por usuarios o por terceros.

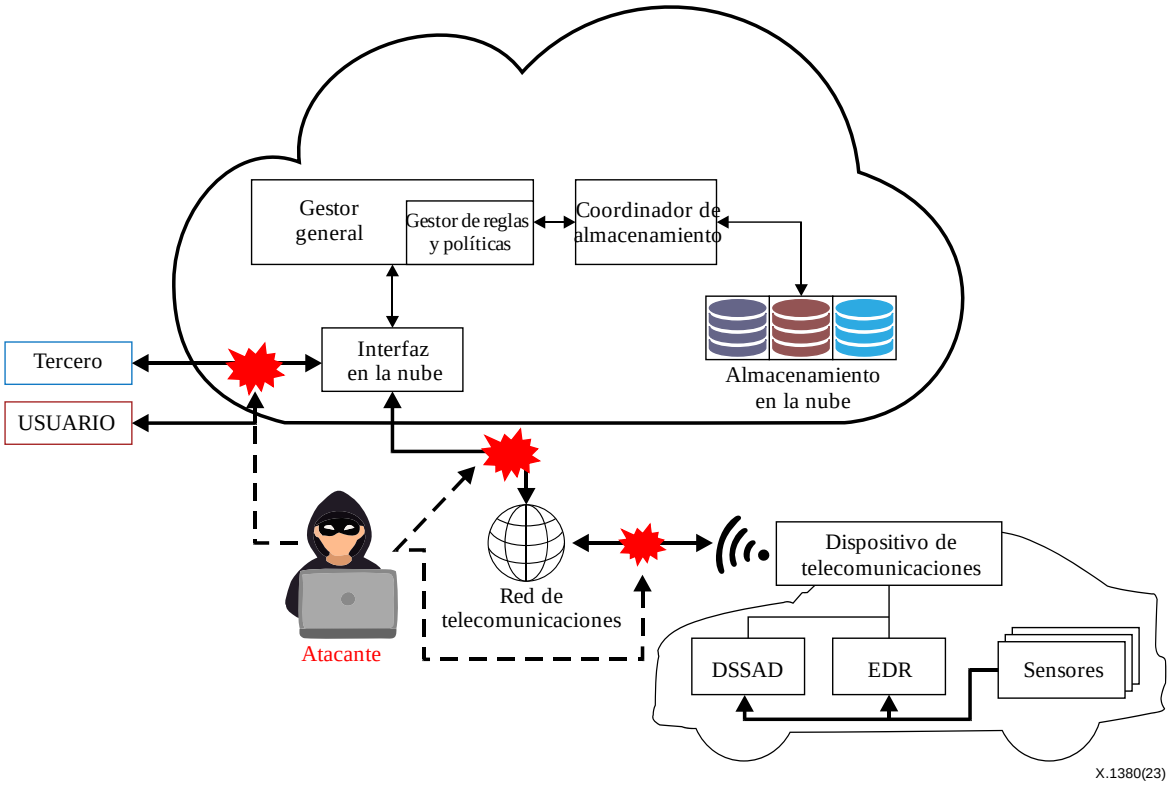

Figura 9 – Escucha clandestina de sistemas de grabación de datos basados en la nube

En tercer lugar, un atacante puede capturar y analizar los datos OTA transmitidos para actualizar las reglas del EDR. De esta forma, el atacante puede enviar reglas falsas para comprometer las medidas de seguridad.

– **Escucha por interceptación**: Una forma de ataque físico es la intervención directa en la red del vehículo. Los vehículos modernos tienen múltiples buses de red de área de controlador (CAN); el acceso a cualquier bus está estrictamente controlado por una pasarela de seguridad (o cortafuegos del vehículo). Los atacantes no pueden observar el tráfico de todos los buses CAN sin disponer de los privilegios de acceso a la pasarela de seguridad. En consecuencia, los atacantes pueden intentar acceder al vehículo objetivo mediante una interceptación física que les permita espiar todo el tráfico de los buses CAN, incluidos los datos EDR/DSSAD.

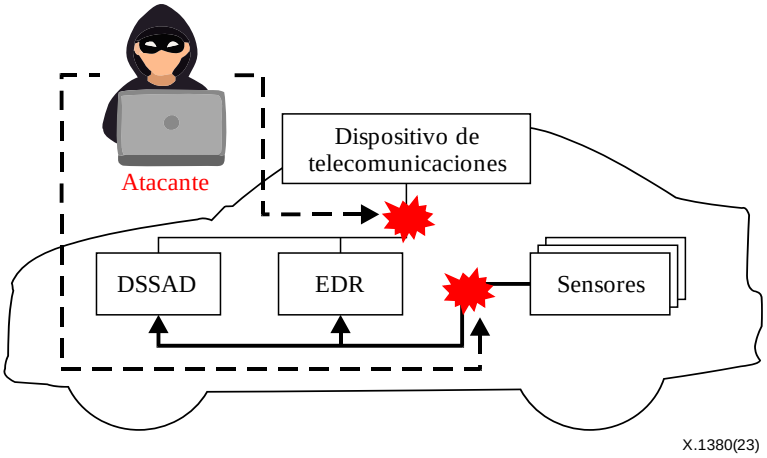

Figura 10 – Interceptación en sistemas de grabación de datos basados en la nube

8.2.2 Amenazas a la integridad

Los datos EDR se utilizan para el análisis de colisiones o accidentes de vehículos, y los datos DSSAD para conocer sobre quién recae la responsabilidad. Por lo tanto, debe garantizarse que los datos no se alteren durante su almacenamiento y tránsito. La integridad es uno de los objetivos de seguridad más importantes de los registros de auditoría, como son los datos EDR/DSSAD. Los atacantes intentan comprometer la integridad de los datos EDR/DSSAD mediante los métodos que se indican a continuación.

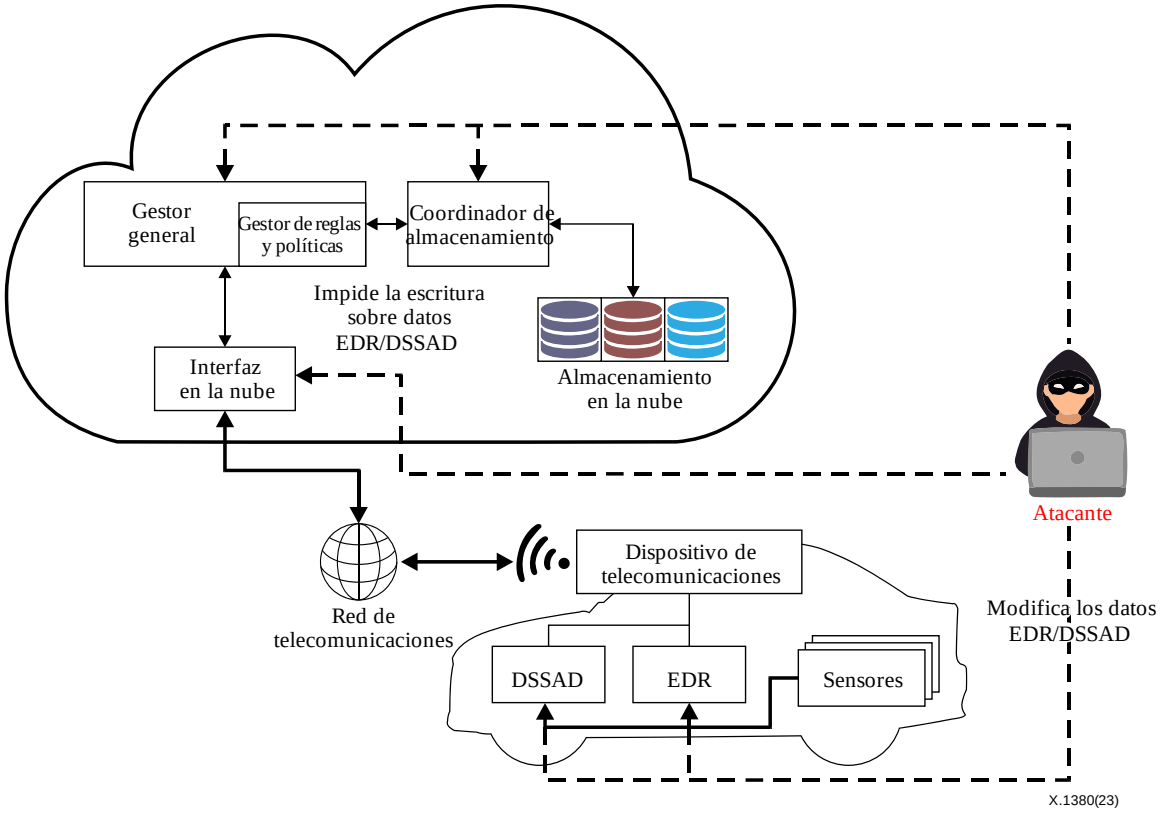

Figura 11 – Manipulación del flujo de control en sistemas de grabación de datos basados en la nube

Al manipular el flujo de control de un sistema de grabación de datos basado en la nube, un atacante podría alterar los datos EDR/DSSAD o impedir la escritura de las entradas de datos EDR/DSSAD. Por ejemplo, el atacante puede identificar y acceder a la interfaz de depuración en la placa de circuito impreso (PCB) del EDR/DSSAD y utilizar esta interfaz para manipular el código ejecutable. Además, un atacante puede manipular el firmware o las reglas del EDR/DSSAD en el EDR/DSSAD. El atacante también puede modificar el tráfico del bus y manipular el registro del EDR/DSSAD.

En el caso del sistema en la nube, el atacante puede acceder al almacenamiento y manipular los datos EDR, los registros de auditoría y la política en la nube utilizando malware e interfaces de programación de aplicaciones (API) inseguras.

La Figura 11 muestra el ataque de manipulación del flujo de control de un sistema de grabación de datos basado en la nube.

8.2.3 Amenazas a la autenticidad

El ataque por intermediario, el ataque por suplantación y repetición son amenazas típicas a la autenticidad.

– **Ataque por intermediario**: En un sistema de grabación de datos basado en la nube, un atacante puede interceptar los mensajes que se transmiten entre un vehículo y la nube o entre la nube y un usuario, y retransmitirlos posteriormente manipulando los mensajes arbitrariamente. El emisor no reconoce que el receptor es un atacante desconocido que trata de acceder o modificar los mensajes antes de retransmitirlos al receptor. Así, el atacante puede controlar toda la comunicación entre ambos.

– **Ataque por suplantación**: En un sistema de grabación de datos basado en la nube, el ataque por suplantación de identidad puede realizarse de cuatro maneras**:**

- Petición falsa de recuperación de datos EDR/DSSAD al sistema en la nube
- Petición falsa al sistema en la nube para actualizar las reglas de un vehículo designado
- Petición de almacenamiento de datos EDR/DSSAD falsos en el sistema en la nube
- Actualización de reglas falsas en el sistema EDR/DSSAD del vehículo

Los ataques de suplantación de identidad pueden causar graves daños a la integridad de todo el sistema de grabación de datos basado en la nube, ya que pueden generar datos de eventos falsos o modificar reglas y políticas relativas a eventos. Además, un ataque de suplantación permite a un atacante filtrar datos privados almacenados en el sistema en la nube.

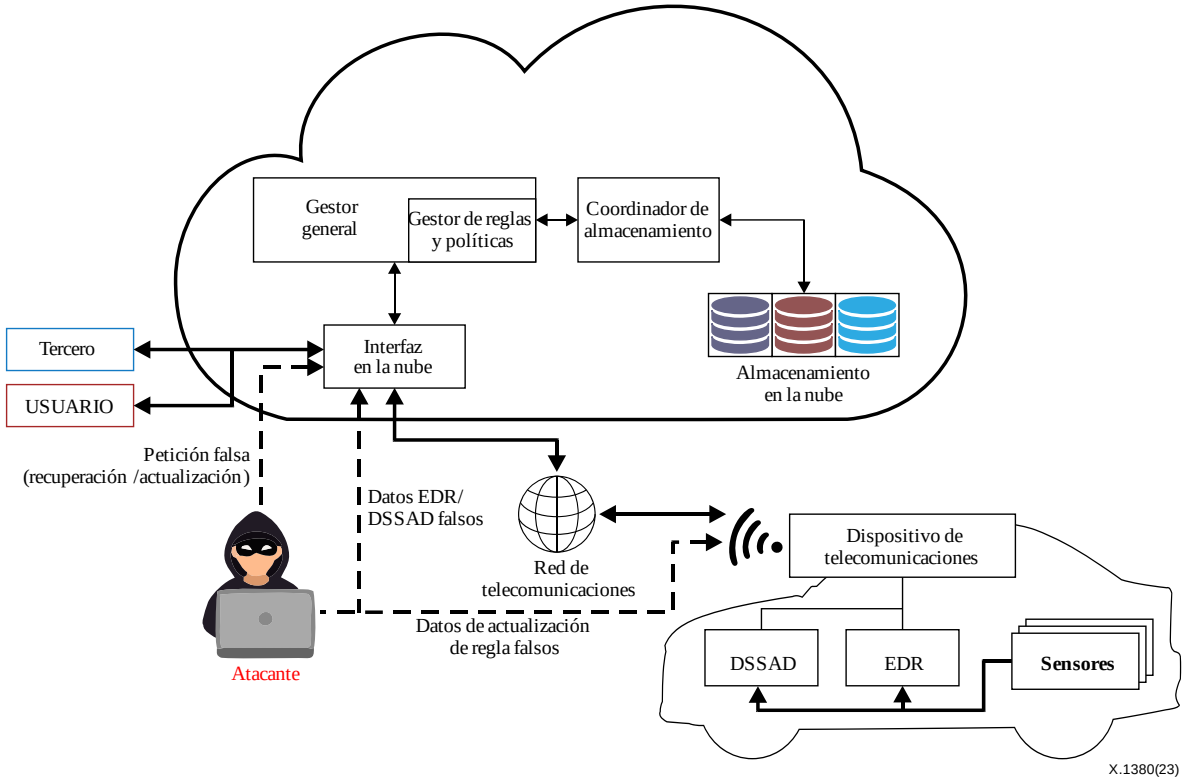

Figura 12 – Ataque por suplantación en sistemas de grabación de datos basados en la nube

– **Ataque por repetición**: un ataque por repetición puede producir la duplicación de datos EDR/DSSAD y la anulación indeseada de reglas o políticas.

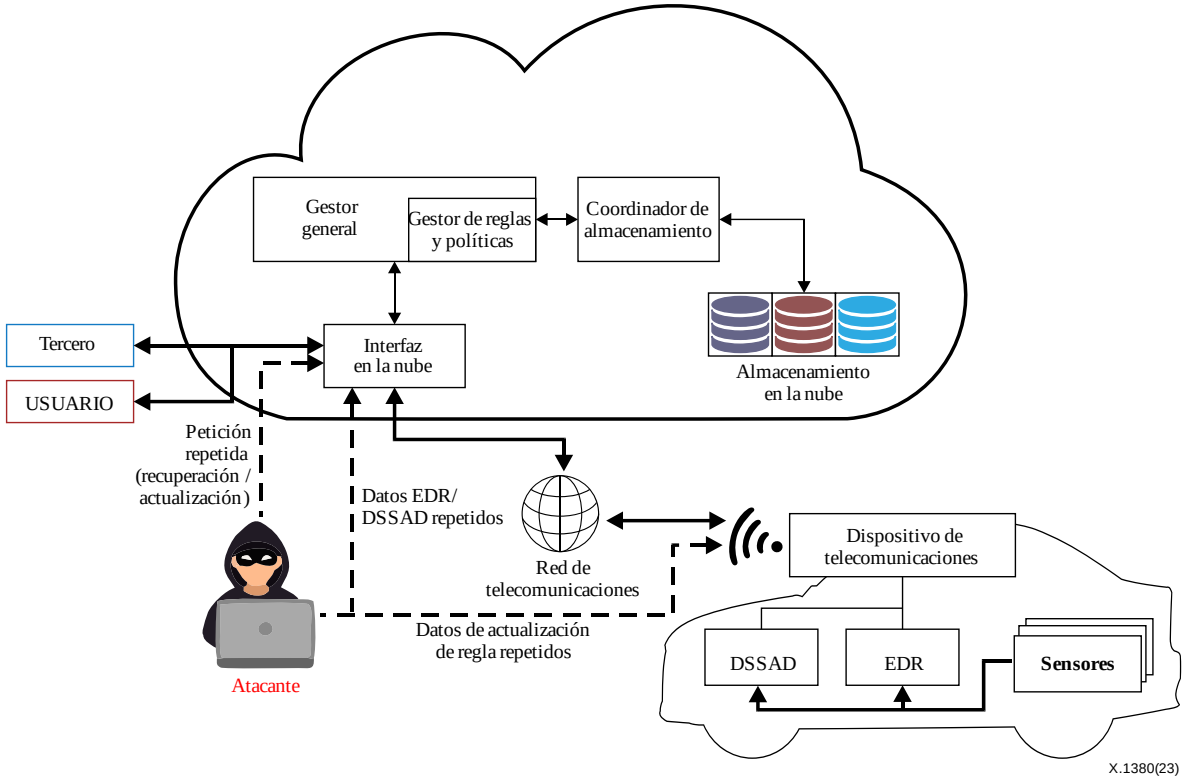

Figura 13 – Ataque por repetición en sistemas de grabación de datos basados en la nube

– **Acceso físico**: Si el atacante puede acceder al vehículo a través del puerto de depuración, puede realizar otros tipos de ataques. La interfaz más comúnmente utilizada como puerto de depuración es el grupo de acción de prueba conjunta (JTAG). El acceso a través de JTAG ofrece la posibilidad de leer y escribir en la memoria, lo que permite manipular el firmware y comprometer las medidas de seguridad.

  Otro acceso físico al vehículo es el de diagnóstico. Un atacante puede acceder al puerto OBD-II utilizando herramientas de diagnóstico o directamente a través de una pasarela que tenga funciones de diagnóstico a distancia. El servicio de diagnóstico unificado (UDS) es un protocolo estándar de diagnóstico que permite monitorizar y manipular la red del vehículo y sus unidades de control electrónicas (ECU).

8.2.4 Amenazas a la disponibilidad

La disponibilidad es un factor crítico de un sistema de grabación de datos basado en la nube, dada la necesidad que puede existir en cualquier momento de almacenar información útil sobre accidentes o colisiones. La amenaza a la disponibilidad más conocida es el ataque de denegación de servicio (DoS).

– **Ataque de denegación de servicio (DoS)**: Los ataques DoS pueden tener graves consecuencias para los sistemas de grabación de datos en la nube, ya que un atacante intenta bloquear los principales sistemas de comunicación, almacenamiento o gestión de datos EDR/DSSAD, lo que anula la funcionalidad del sistema de grabación de datos basado en la nube para el análisis de accidentes. A título de ejemplo de ataque DoS, la inundación del canal de la red con un elevado volumen de mensajes generados por un atacante puede paralizar los nodos de la red o los sistemas completos en la nube. Los nodos de la red (en el vehículo o en el sistema en la nube) no pueden manejar la enorme cantidad de datos recibidos, lo cual provoca un mal funcionamiento del almacenamiento de los datos EDR/DSSAD en los sistemas en la nube o la actualización de las reglas o políticas intravehiculares y de los sistemas en la nube.

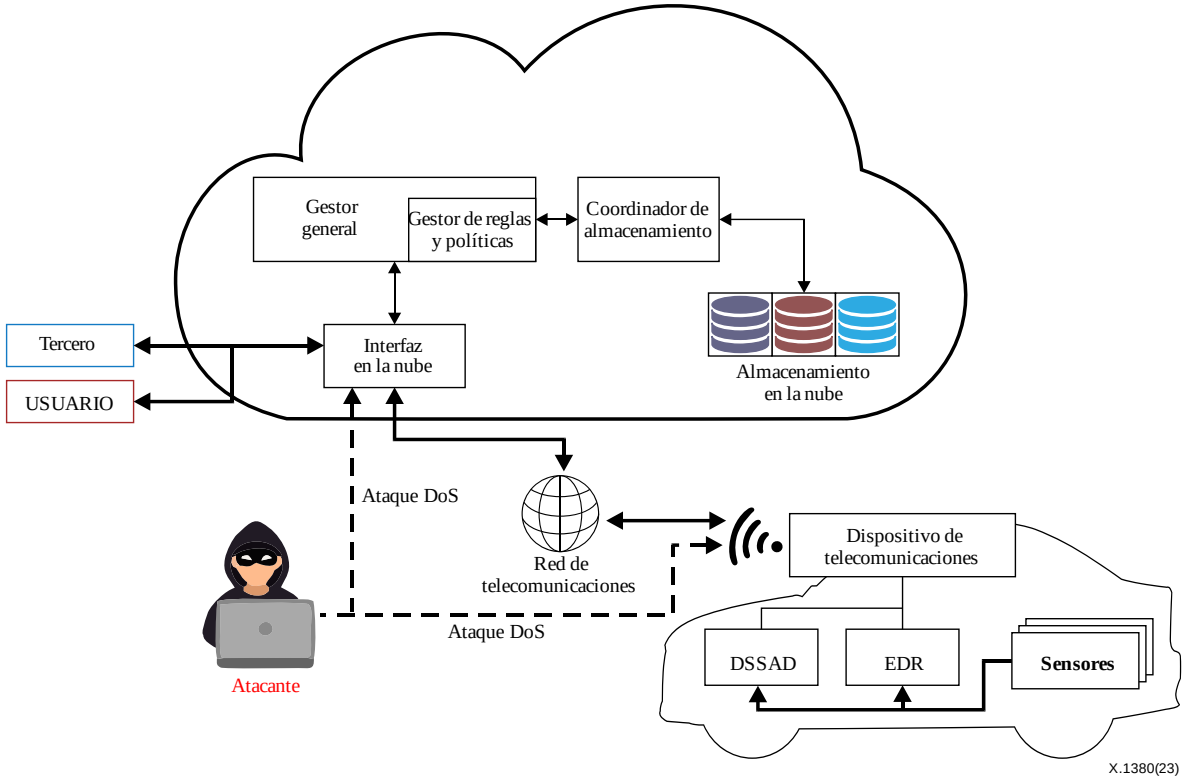

Figura 14 – Ataque DoS a sistemas de grabación de datos basados en la nube

8.2.5 Amenazas a la identificación de responsabilidades

– **Pérdida de la trazabilidad de los eventos**: Los componentes como el gestor de reglas y políticas y el coordinador de almacenamiento incluidos en el sistema en la nube, funcionan de acuerdo con el conjunto de reglas y políticas que instala el usuario que tiene la autoridad para ello. Por lo tanto, la gestión del registro de cambio de las reglas y las políticas es muy importante en términos de identificación de responsabilidades. Un atacante puede crear confusión manipulando o borrando el registro de eventos

9 Requisitos de seguridad

9.1 Carga segura

Se recomienda comprobar la integridad del firmware almacenado en la memoria de los dispositivos EDR/DSSAD antes o durante su ejecución. También se recomienda comprobar la integridad de las reglas del EDR/DSSAD y de los datos de configuración y calibración conexos.

El proceso de protección del firmware y las reglas consta de dos pasos. En primer lugar, durante la instalación del firmware y las reglas, se comprueba su autenticidad antes de que ser grabados en la memoria interna y se configuren como el firmware y las reglas actuales. En segundo lugar, durante cada arranque, se comprueba la integridad del firmware y las reglas actuales.

Se recomienda que el mecanismo de arranque seguro emplee medios criptográficos simétricos o asimétricos para verificar la integridad del firmware y las reglas aplicando niveles adecuados de seguridad. También se recomienda que los dispositivos EDR y DSSAD utilicen un hardware que actúe como ancla de confianza, como un módulo de seguridad del hardware (HSM) para almacenar las claves criptográficas de forma segura y acelerar el cálculo de los algoritmos criptográficos.

9.2 Registro seguro

Se deberá garantizar la integridad de los datos de registro utilizando métodos criptográficos seguros. Dado que los datos EDR/DSSAD son elementos de prueba para situaciones específicas, los datos EDR/DSSAD deben estar protegidos frente a manipulaciones no autorizadas.

En el caso del sistema en la nube, el sistema de gestión general debe incluir registros para cada uno de los casos siguientes:

– Intentos de autenticación de usuarios o terceros.

– Actualización de la política.

Se recomienda que los registros se almacenen de forma segura. Se pueden añadir medidas criptográficas a los registros, como códigos de autenticación de mensajes (MAC) y almacenarlos de forma mediante un control de acceso adecuado. La retención mínima de los registros debe definirse siguiendo la política del proveedor de servicios en la nube o la reglamentación nacional.

9.3 Comunicación segura

Los sistemas de grabación de datos basados en la nube tienen varios canales de comunicación, tal como se indica a continuación:

– Comunicación entre los sistemas en la nube y los vehículos.

– Comunicación entre usuarios y terceros.

– Comunicación entre unidades de control electrónico (ECU) y actuadores a bordo de vehículos.

Se recomienda garantizar la confidencialidad y autenticidad de los mensajes de comunicación entre el sistema en la nube y los vehículos o usuarios/terceros. La confidencialidad y la autenticidad pueden lograrse con medidas criptográficas como la seguridad de la capa de transporte (TLS).

También se recomienda que la comunicación entre el sistema en la nube y el vehículo garantice la disponibilidad. Esto significa el almacenamiento en la nube de una enorme cantidad de datos EDR y DSSAD de numerosos vehículos en una forma apropiada.

Se recomienda garantizar la integridad de los mensajes y los datos en las comunicaciones entre las ECU, los sensores y los actuadores de los vehículos para generar datos EDR/DSSAD correctos, dado que los datos de las ECU y de los sensores están relacionados con eventos de colisión o las actividades de conducción.

9.4 Acceso seguro

Se recomienda deshabilitar en el dispositivo EDR/DSSAD las interfaces de depuración, como JTAG, que no sean obligatorias para el funcionamiento normal, y no debe obviar el arranque seguro. Los métodos de desactivación de la interfaz de depuración se clasifican de la forma siguiente:

– Supresión permanente.

– Inhabilitación condicional mediante control de acceso.

En el caso de volver a habilitar las interfaces de depuración en el caso de un análisis para retomar la garantía, sólo partes autorizadas y autenticadas podrán acceder a las interfaces de depuración. Se recomienda limitar los privilegios de las aplicaciones que acceden a través de las interfaces de hardware y software conforme al principio de privilegios mínimos.

Se recomienda proteger mediante un mecanismo criptográfico las funciones y datos críticos para la seguridad que emplean comandos y solicitudes de diagnóstico. Esto conlleva la necesidad de autenticación del sujeto que desee acceder al dispositivo EDR/DSSAD antes de la transmisión de comandos.

9.5 Actualización segura

Se recomienda garantizar la autenticidad e integridad del procedimiento de actualización del firmware y de las reglas, es decir, que sólo se permita la incorporación de paquetes de actualización autentificados y no alterados. Además, se recomienda no migrar el firmware y las reglas a una versión anterior para evitar el uso malicioso de antiguas vulnerabilidades de seguridad. También se recomienda que los paquetes OTA se transmitan a través de un canal seguro protegido por métodos criptográficos.

9.6 Relación entre las amenazas identificadas y los requisitos de seguridad

El Cuadro 3 proporciona información sobre la correspondencia existente entre las amenazas identificadas en la cláusula 8 y los requisitos de seguridad.

Cuadro 3 – Relación entre las amenazas identificadas y los requisitos de seguridad

Requisitos de seguridad	Amenazas	Objetivos de seguridad
Arranque seguro	Manipulación del flujo de control – manipulación del firmware – manipulación de las reglas del EDR/DSSAD	Integridad de las reglas del EDR/DSSAD almacenadas en los vehículos Integridad del firmware de EDR/DSSAD
Registro seguro	Manipulación del flujo de control – manipulación de los registros Pérdida de la trazabilidad de los eventos	Integridad de los datos EDR/DSSAD en los vehículos. Integridad del registro en la nube
Comunicación segura	Escucha clandestina Escucha por interceptación Manipulación del flujo de control Ataque por intermediario Ataque por suplantación Ataque por repetición Ataque DoS	Confidencialidad y/o integridad del tráfico del bus Confidencialidad y autenticidad de la comunicación con los sistemas de soporte Disponibilidad de los sistemas soporte
Acceso seguro	Acceso físico	Confidencialidad y/o autenticidad de la comunicación con la depuración y el diagnóstico
Actualización segura	Escucha clandestina Manipulación del flujo de control – manipulación de reglas EDR/DSSAD Ataque por suplantación	Confidencialidad e integridad del paquete OTA

10 Directrices para la implementación de sistemas de grabación de datos basados en la nube

El uso y la gestión de datos EDR/DSSAD requiere la protección de los sistemas de grabación de datos asados en la nube. Los sistemas de grabación de datos basados en la nube aportan también funcionalidades para la investigación y el desarrollo de vehículos más seguros mediante el uso de datos grabados que no pueden proporcionar los sistemas de grabación de datos convencionales. Esta cláusula incluye directrices para la implementación de un sistema de grabación de datos basado en la nube.

10.1 Separación del almacenamiento en la nube

Debido al carácter esencial de la VII en un sistema EDR/DSSAD basado en la nube, esta deberá estar protegida. En los sistemas EDR/DSSAD basados en la nube, los datos EDR/DSSAD y su correspondiente VII deberán estar físicamente separados. Eso no sólo trae consigo beneficios de seguridad, sino que permite realizar funciones adicionales como proporcionar datos EDR/DSSAD de terceros sin violar la privacidad. El almacenamiento debe estar físicamente separado y gestionado de forma independiente en distintos sistemas de almacenamiento. Dada su importancia relativa, el almacenamiento de la VII (descrito como base de datos de VII en la Figura 15) requiere un nivel de seguridad más elevado que otros datos.

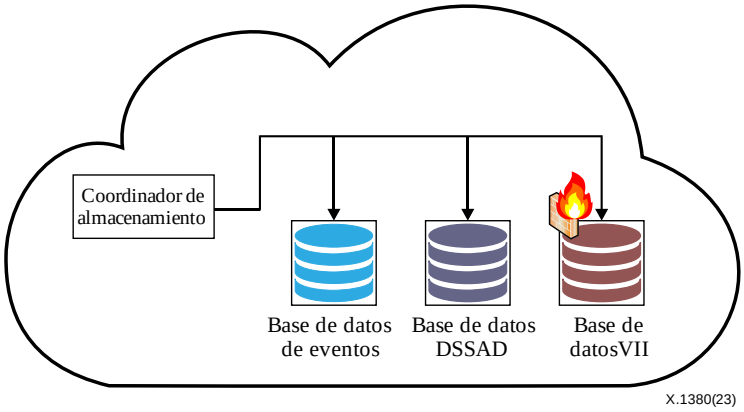

Figura 15 – Separación del almacenamiento

10.1.1 Procedimiento de almacenamiento de los datos

Para garantizar la confidencialidad y autenticidad de los datos de la comunicación con un sistema soporte, es necesario establecer un canal seguro antes de transmitir los datos EDR/DSSAD desde un vehículo al sistema en la nube.

Cuando se entregan los datos al coordinador de almacenamiento desde un vehículo a través de una interfaz en la nube, el coordinador de almacenamiento separa los datos EDR/DSSAD y la VII. Tras la separación, el coordinador genera los datos de enlace que permitirían combinar de nuevo los datos EDR/DSSAD con los datos VII. A continuación, los dos conjuntos de datos se almacenan por separado en distintos almacenes (bases de datos). Tal como se describe en la Figura 16, los datos VII y EDR/DSSAD se almacenan, junto con los datos del enlace, en la base de datos VII y en la base de datos de eventos/DSSAD respectivamente. Una vez realizado el almacenamiento, se debe registrar el resultado, es decir, el éxito o fracaso del procedimiento de almacenamiento de datos.

Uno de los aspectos más importantes de los procedimientos de almacenamiento de datos es el cumplimiento de la reglamentación pertinente, como el Reglamento General de Protección de Datos (RGPD). Por lo tanto, antes de recopilar cualquier dato del vehículo se recomienda obtener el consentimiento del propietario de los datos.

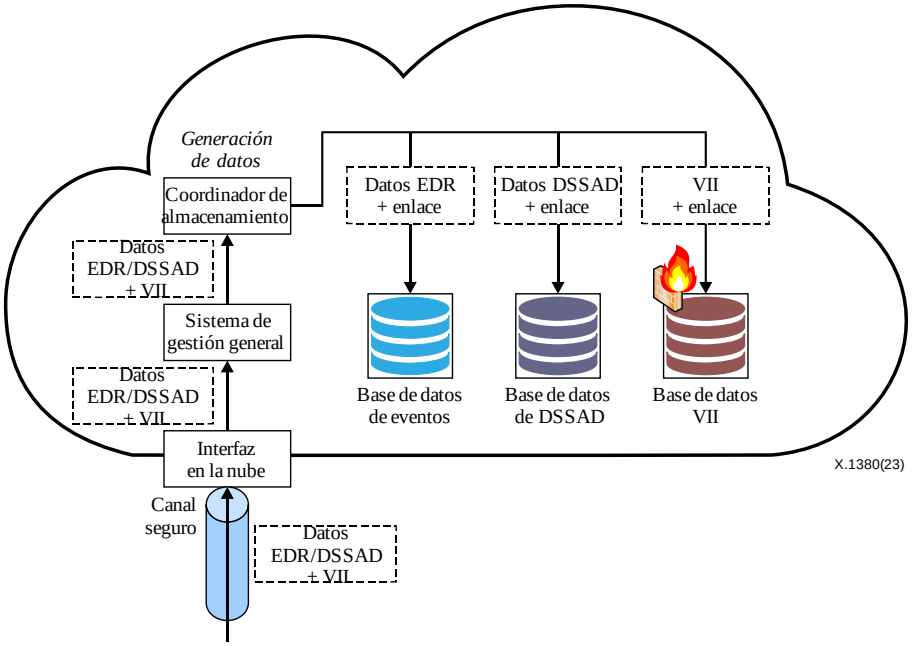

Figura 16 – Procedimiento de almacenaje para almacenamiento separado

10.1.2 Procedimiento de recuperación de datos

El procedimiento de recuperación de datos EDR/DSSAD comienza con la petición de recuperación de los datos por el usuario o un tercero. Cuando el usuario o el tercero accede al sistema en la nube, la interfaz en la nube debe autenticarlo y registrar todos los intentos. Si la autenticación tiene éxito, el coordinador de almacenamiento utiliza la VII presentada para encontrar los datos de enlace en la base de datos de VII (véase la Figura 17 a)). Utilizando los datos de enlace encontrados, el coordinador de almacenamiento busca los datos EDR/DSSAD. Cuando los encuentra, el coordinador de almacenamiento proporciona los datos al solicitante, teniendo en cuenta que el procedimiento de control de acceso del sistema general de gestión difiriere según el nivel de la autorización del solicitante. Para la recuperación de datos VII podrá hacerse de forma restrictiva y se requiere una autorización de alto nivel. Por otro lado, un tercero puede recuperar los datos EDR o DSSAD que no incluyan VII. Los datos EDR o DSSAD pueden recuperarse sin aplicar el proceso de búsqueda de la VII cuando los datos VII se eliminan y se transfieren a un servidor neutro separado (véase la Figura 17 b)).

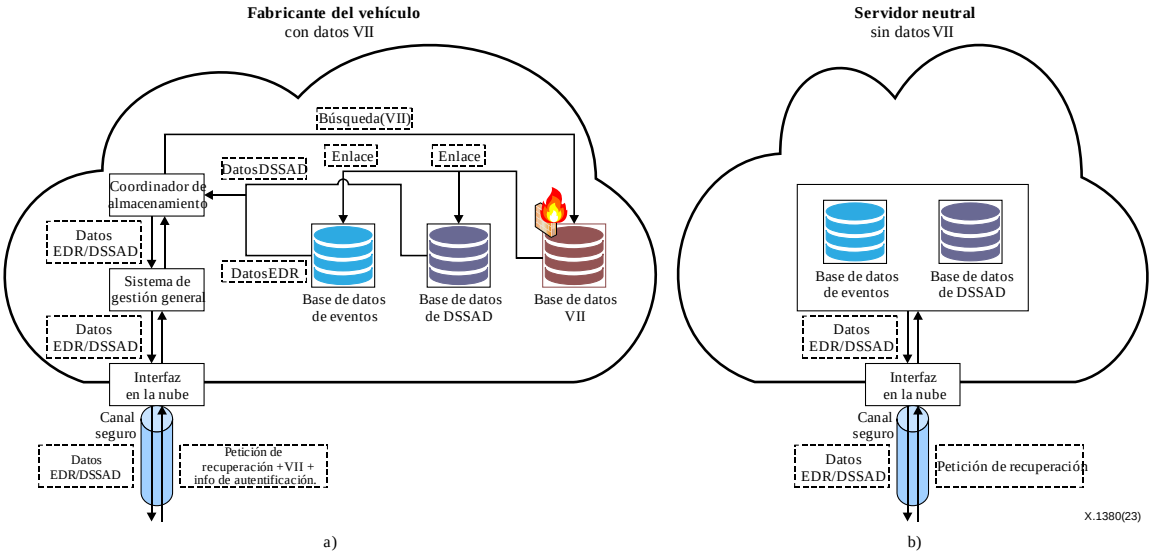

Figura 17 – Procedimiento de recuperación del almacenamiento por separado

10.1.3 Procedimiento de eliminación de datos

El sistema en la nube para EDR/DSSAD debe tener el consentimiento del usuario, incluyendo la fecha de caducidad o la duración de los datos grabados de los datos VII recopilados. Cuando se alcanza la fecha de caducidad o se supera la duración máxima de los datos almacenados, los datos recogidos deben ser eliminados automáticamente del sistema en la nube.

Cuando los usuarios solicitan la eliminación de sus datos antes de la fecha de caducidad, los sistemas en la nube deben eliminar los datos con arreglo a la solicitud. Cuando un usuario solicita la eliminación, la interfaz en la nube debe autenticar al usuario y registrar todos los intentos. Si la autenticación tiene éxito, el coordinador de almacenamiento debe utilizar la VII presentada para encontrar los datos de enlace almacenados en la base de datos de VII. El coordinador de almacenamiento debe buscar los datos EDR/DSSAD utilizando para ello los datos de enlace encontrados y borrarlos una vez encontrados. A continuación, el coordinador de almacenamiento debe almacenar el registro relativo al resultado de la eliminación e informar del mismo a la parte solicitante.

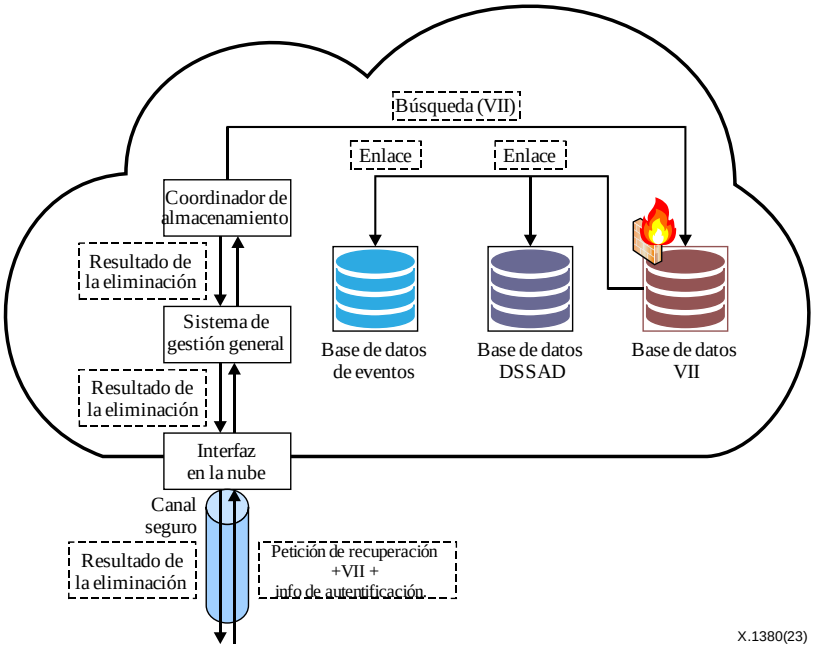

Figura 18 – Procedimiento de supresión del almacenamiento por separado

10.2 Registro del servicio en la nube

En la Figura 19 se muestra el procedimiento de registro de los sistemas de grabación de datos basados en la nube en entornos automovilísticos.

Como se observa en la Figura 19, si se recibe de un vehículo una solicitud de autentificación para el registro de un servicio de grabación de datos basado en la nube en el modo ejecución de servicio del paso 1, es decir, una solicitud de autentificación del vehículo se debe verificar el ID del vehículo, por ejemplo, utilizando un algoritmo de firma digital de un sistema criptográfico de clave pública del paso 2. En este caso, la solicitud de autentificación del vehículo puede realizarse mediante la transmisión de un mensaje firmado con la clave privada del vehículo dirigido al sistema de servicio de grabación de datos basado en la nube. Si tras la verificación del paso 2, se determina que el ID del vehículo es inválido, el sistema del servicio de grabación de datos basado en la nube genera la correspondiente respuesta de fallo de autentificación y la transmite al vehículo, como se muestra en el paso 3.

Si tras la verificación del paso 2, se determina que el ID del vehículo es válido, el sistema del servicio de grabación de datos basado en la nube genera una respuesta de autentificación y la transmite al vehículo, como se muestra en el paso 4.

A continuación, cuando se recibe la respuesta de autentificación, es decir, cuando el vehículo se autentifica después de que el usuario presenta y genera la información de registro del servicio de grabación de datos basado en la nube, incluidos los tipos de datos y el periodo de grabación, etc., el vehículo transmite la información de registro del servicio de grabación de datos en la nube al sistema del servicio de grabación de datos en la nube para , de ese modo, solicitar el registro del servicio de grabación de datos en la nube, tal como se muestra en el paso 5.

Consiguientemente, si se recibe una solicitud de registro del servicio de grabación de datos basado en la nube, que incluye la información de registro del servicio de grabación de datos en la nube, el sistema del servicio de grabación de datos en la nube genera una política de seguridad utilizando la información de registro del servicio de grabación de datos en la nube, como son los tipos de datos de la grabación y el periodo de grabación y así sucesivamente, y a continuación almacena y registra la información, como se muestra en el paso 6.

A partir de ahí, el sistema del servicio de grabación de datos basado en la nube asigna un seudónimo a cada vehículo, como se muestra en el paso 7, genera un mensaje de solicitud de certificado para solicitar la generación de un certificado de seudónimo para el seudónimo asignados a cada vehículo y transmite el mensaje de solicitud de certificado al centro de autentificación, como se muestra en el paso 8.

El sistema del servicio de grabación de datos basado en la nube verifica, en el paso 9, si se ha obtenido el certificado de seudónimo del centro de autentificación. Si se verifica el certificado del seudónimo, el sistema del servicio de grabación de datos en la nube almacena el certificado en la base de datos de información de la grabación de datos en la nube. El certificado de seudónimo puede ser un mensaje firmado digitalmente recibido del centro de autentificación. Es posible garantizar la justificación del seudónimo mediante el certificado de seudónimo.

Cada vehículo puede recibir varios seudónimos. Dado que el seudónimo carece de información asociada con el ID del vehículo, se puede proteger la IIP de cada vehículo.

Si se recibe la notificación, en el paso 10 el sistema del servicio de grabación de datos basado en la nube genera la información de registro del servicio de grabación de datos en la nube de cada vehículo, almacena la base de datos de información y la transmite a cada uno de los vehículos. Esta información de registro del servicio de grabación de datos en la nube puede contener un seudónimo asignado a cada vehículo, los certificados de dichos seudónimos, etc. Cada vehículo, es decir, el usuario de cada vehículo registrado en el servicio de grabación de datos en la nube puede realizar la grabación de los datos en la nube estableciendo previamente la comunicación pertinente entre vehículo y el centro en la nube utilizando la información de registro del servicio de grabación de datos en la nube facilitado por el sistema del servicio de grabación de datos basado en la nube.

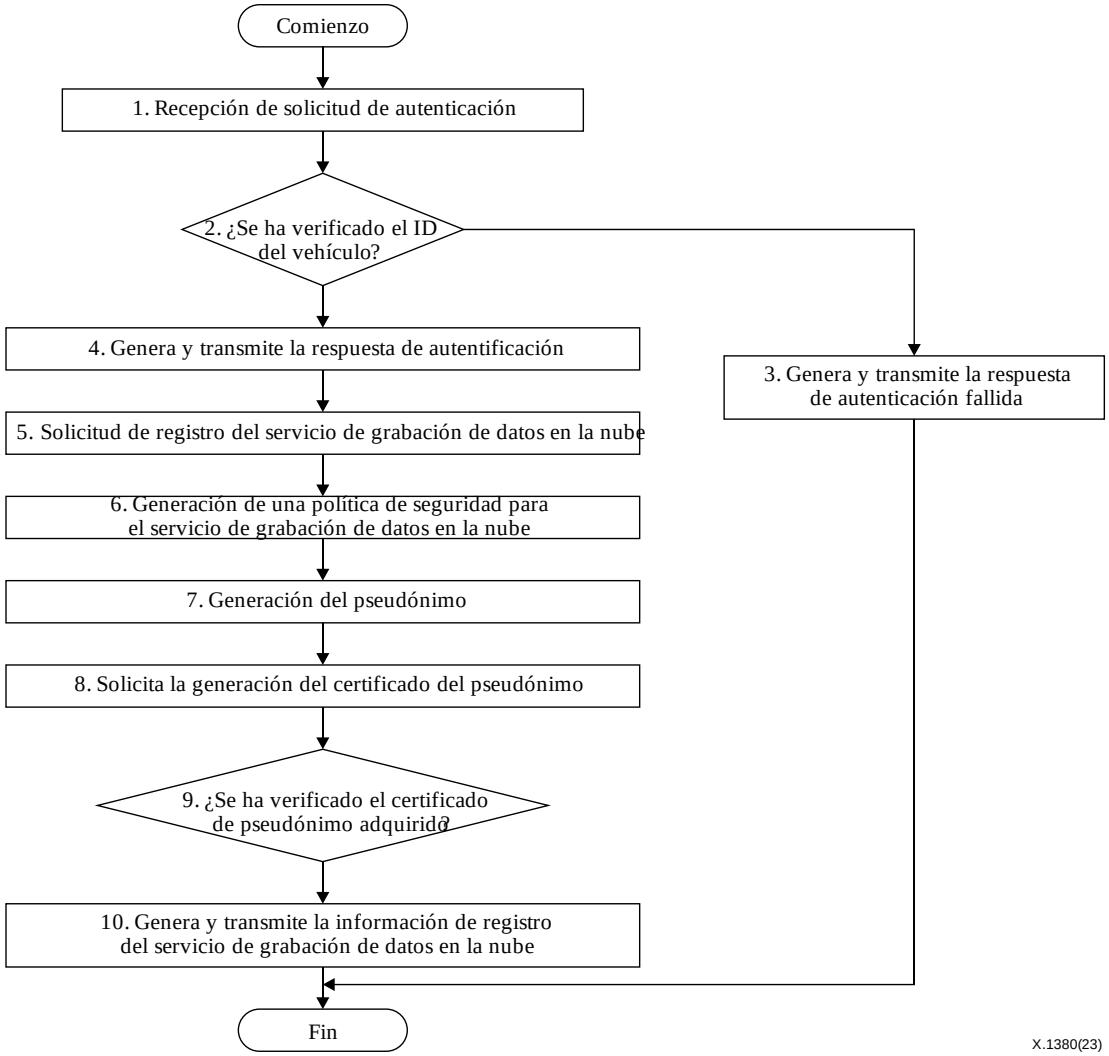

Figura 19 – Registro del servicio de grabación de datos en la nube

Para determinados casos de uso, se puede considerar el procedimiento de baja de sistemas de grabación de datos basados en la nube, por ejemplo, para el alquiler de vehículos, los vehículos usados, etc., cuando los nuevos propietarios no deseen proporcionar datos EDR/DSSAD al sistema en la nube.

11 Casos de uso de sistemas de grabación de datos basados en la nube en un entorno automovilístico

Cuando se produce un accidente de tráfico, los datos del EDR/DSSAD son importantes para analizar la causa del accidente y determinar si el vehículo y el conductor son responsables. La Figura 20 muestra el flujo de datos EDR/DSSAD. Los datos EDR/DSSAD generados en el vehículo se transmiten a la nube por medios radioeléctricos. El propietario del vehículo, el fabricante, los proveedores o los terceros autorizados (por ejemplo, las compañías de seguros) pueden utilizar los datos EDR/DSSAD en la nube.

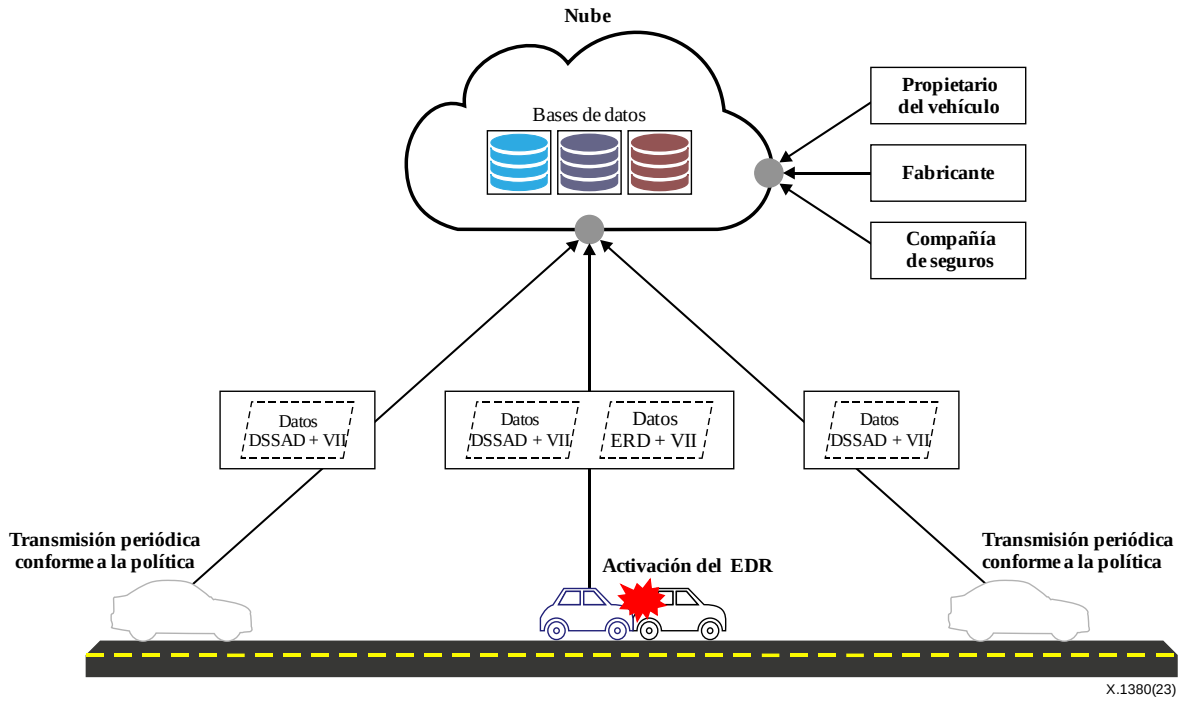

Figura 20 – Flujo de datos EDR/DSSAD

Un sistema de grabación de datos basado en la nube tiene muchas ventajas. En primer lugar, es fácil obtener datos EDR/DSSAD, incluso en situaciones de riesgo potencial (por ejemplo, incendios de vehículos, inundaciones de vehículos). En segundo lugar, los analistas de accidentes autorizados pueden tomar los datos del sistema en la nube más fácilmente que directamente a través de las ECU del vehículo.

11.1 Caso 1: Colisión entre vehículos

La Figura 21 muestra un caso de cronología en el que un vehículo equipado con un sistema automatizado de mantenimiento de carril (ALKS) circula por la carretera. El accidente de tráfico se produce en el punto (e) lo que desencadena un evento EDR. La nube almacena los datos EDR/DSSAD desde (a), cuando se activa el ALKS, hasta (e), cuando se produce el accidente. Los datos EDR/DSSAD almacenados aportan la información siguiente:

A partir de que el conductor activa el ALKS a las 10:19:10, se transfiere el control del vehículo al sistema. Al cabo de 1 minuto y 50 segundos, el tiempo empeora y el ALKS pide al conductor que retome el control del vehículo, pero éste no responde. El ALKS inicia entonces automáticamente una maniobra de riesgo mínimo (MRM) a las 10:22:00. La colisión se produce a las 10:22:30.

Mediante el análisis de los datos EDR/DSSAD, es posible comprobar el periodo y las circunstancias en las que se produjo el accidente. Los sistemas de grabación de datos basados en la nube almacenan los datos EDR/DSSAD en el sistema en la nube mediante políticas de transferencia de datos predefinidas. De este modo, se reducen los esfuerzos para la recopilación de información de un accidente en comparación con la recuperación directa de lo almacenado en el EDR del vehículo.

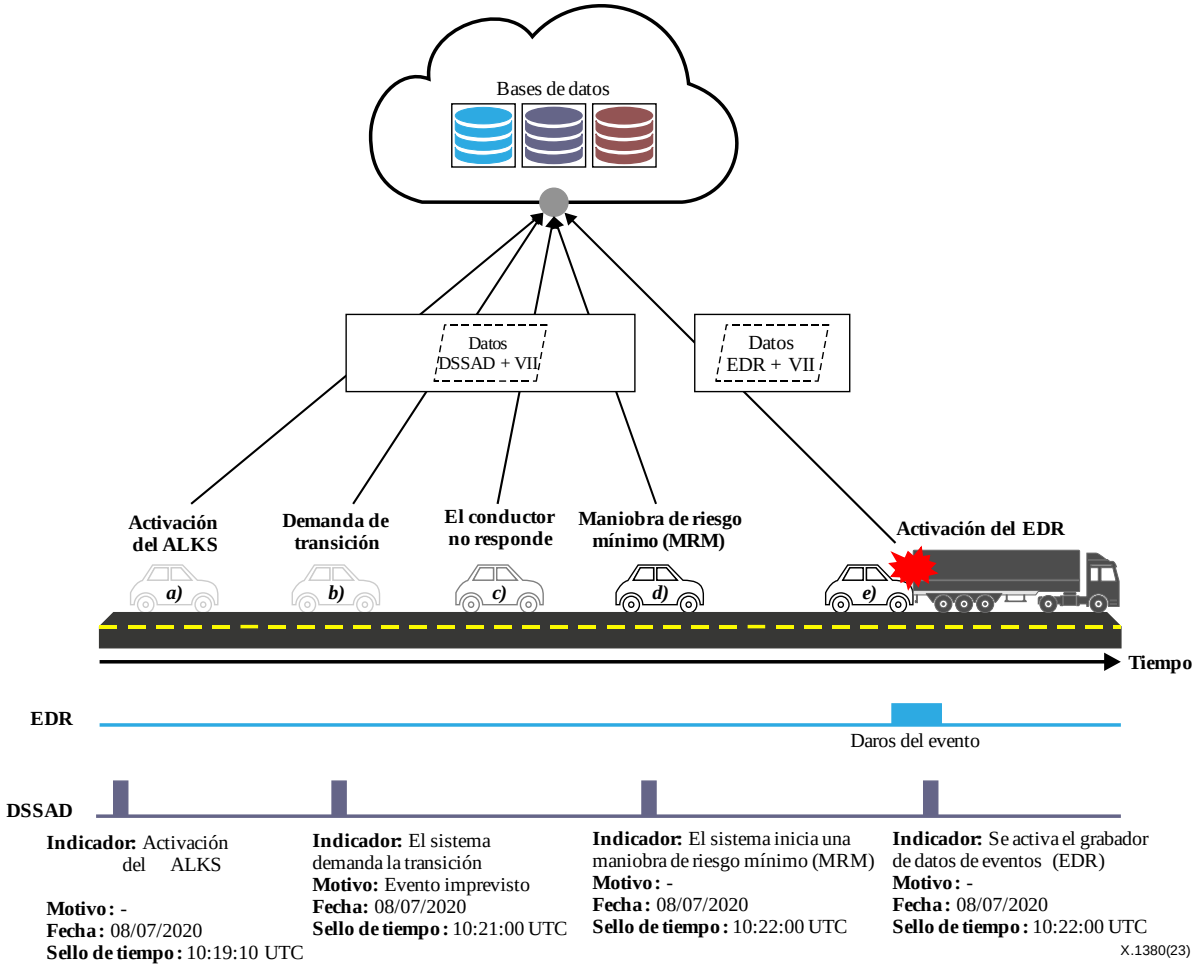

Figura 21 – Colisión entre vehículos

11.2 Caso 2: Colisión entre un vehículo y una bicicleta

La Figura 22 muestra la cronología de un caso en el que un vehículo equipado con un ALKS circula por la carretera. El vehículo tiene una colisión menor con una bicicleta en (c), pero como el impacto es bastante débil el EDR no se activa. Sin embargo, todos los datos DSSAD recientes se suben a la nube. El EDR/DSSAD almacenado reporta la siguiente información:

> El conductor activa el ALKS a las 10:19:10. Transcurridos 15 segundos, el conductor pasa a manejar la dirección personalmente y se desactiva el ALKS. La colisión con la bicicleta ocurre a 07:10:16.

En este caso, el impacto sobre el vehículo es tan leve que no se cumple la condición desencadenante del EDR y no se recogen datos del mismo. No obstante, la situación detallada del accidente se puede simular y analizar fácilmente porque los datos del DSSAD se almacenan en el sistema en la nube.

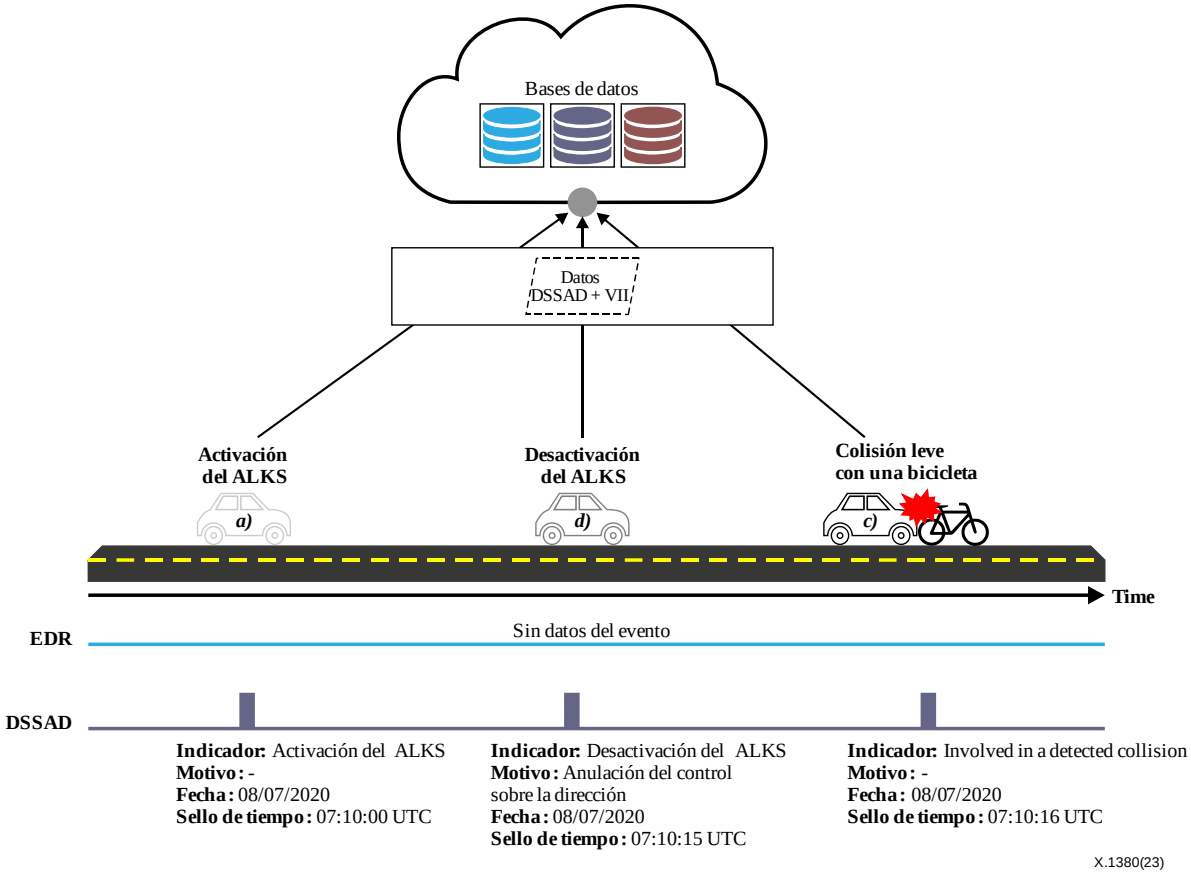

Figura 22 – Colisión entre un vehículo y una bicicleta

Apéndice I

(Este apéndice no forma parte integrante de la presente Recomendación.)

Ejemplo de conjunto de datos de un EDR convencional

Este ejemplo de conjunto de datos es un elemento de datos esencial requerido para los EDR convencionales en los Estados Unidos de América (EE.UU.), que están regulados por la NHTSA (National Highway Traffic Safety Administration).

Cuadro I.1 – Elementos de datos esenciales de un EDR convencional [b-NHTSA EDR]

Número	Elementos de datos	Tiempo de grabación	Velocidad de muestreo	Gama de valores	Precisión	Resolución
1	Delta-V, longitudinal	0-250 ms o desde 0 hasta el final del evento más 30 ms, lo que sea menor	100/s	–100 a 100 km/h	±10%	1 km/h
2	Delta-V máxima, longitudinal	0-300 ms o desde 0 hasta el final del evento más 30 ms, lo que sea menor	N.A.	–100 a 100 km/h	±10%	1 km/h
3	Tiempo, Delta-V máxima, longitudinal	0-300 ms o desde 0 hasta el final del evento más 30 ms, lo que sea menor	N.A.	0-300 ms o desde 0 hasta el final del evento más 30 ms, lo que sea menor	±3 ms	2,5 ms
4	Velocidad, indicación de vehículo	–5,0 a 0 s.	2/s	0-200 km/h	±1 km/h	1 km/h
5	Delta-V, longitudinal	–5,0 a 0 s.	2/s	0 – 100%	±5%	1%
6	Acelerador, % del máximo (% del máximo del pedal acelerador)	–-5,0 a 0 s.	2/s	Activado/desactivado	N.A.	Activado/desactivado
7	Frenos, activados/ desactivados	–1,0 s	N.A.	0-60.000	± 1 ciclo	1 ciclo
8	Ciclo de encendido, colisión	A la hora de la descarga	N.A.	0-60.000	± 1 ciclo	1 ciclo
9	Ciclo de encendido, descarga	–1,0 s	N.A.	Activado/desactivado	N.A.	Activado/desactivado
10	Situación del cinturón de seguridad	–1,0 s	N.A.	Activado/desactivado	N.A.	Activado/desactivado
11	Luz de aviso del airbag frontal	Evento	N.A.	0 – 250 ms	±2 ms	1 ms
12	Tiempo de despliegue del airbag frontal, RFP (1ª etapa en caso de airbags multietapa)	Evento	N.A.	0 – 250 ms	±2 ms	1 ms
13	Múltiples eventos, número de eventos (1 ó 2)	Evento	N.A.	1, 2	N.A.	1, 2
14	Tiempo entre eventos 1 y 2	Según sea necesario	N.A.	0 – 5,0 s	0,1 s	0,1 s
15	Fichero completo grabado (sí o no)	Después de otros datos	N.A.	Sí/No	N.A:	Sí/No

Bibliografía

[b-ITU-T X.641] Recomendación UIT-T X.641 (1997), *Tecnología de la información – Calidad de servicio: margo general.*

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

[b-ITU-T X.1252] Recomendación UIT-T X.1252 (2021), *Términos y definiciones de referencia para la gestión de la identidad.*

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

[b-UN R157] Reglamento N° 157 de las Naciones Unidas, *Disposiciones uniformes relativas a la homologación de los vehículos de motor por lo que respecta al sistema automático de mantenimiento del carril.*

[b-UN R160] Addéndum 159 – Reglamento N° 157 de las Naciones Unidas, *Disposiciones uniformes relativas a la homologación de los vehículos de motor por lo que respecta al registro de datos de eventos.*

[b-NHTSA EDR] NHTSA, *Final regulatory evaluation: Event data recorders (EDRs) (Evaluación reglamentaria final: sistemas de grabación de datos de eventos, EDR).*

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2023