Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.551

(01/2022)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIA

Pasarelas vehiculares y sistemas de transporte inteligentes (STI) – Arquitectura de las pasarelas vehiculares

Arquitectura de sistemas multimedios en vehículos

Recomendación UIT-T H.551

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIA

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
Sistemas y equipos terminales para los servicios audiovisuales	H.300–H.349
Arquitectura de servicios de directorio para servicios audiovisuales y multimedia	H.350–H.359
Arquitectura de la calidad de servicio para servicios audiovisuales y multimedia	H.360–H.369
Telepresencia	H.420–H.429
Servicios suplementarios para multimedia	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedia de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedia	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedia	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedia	H.540–H.549
PASARELAS VEHICULARES Y SISTEMAS DE TRANSPORTE INTELIGENTES (STI)	
Arquitectura de las pasarelas vehiculares	**H.550–H.559**
Interfaces de pasarelas vehiculares	H.560–H.569
SERVICIOS MULTIMEDIOS DE BANDA ANCHA, DE TRÍADA Y AVANZADOS	
Servicios multimedia de banda ancha sobre VDSL	H.610–H.619
Servicios y aplicaciones multimedios avanzados	H.620–H.629
Aplicaciones de red de sensores ubicuos e Internet de las cosas	H.640–H.649
SERVICIOS MULTIMEDIOS Y APPLICACIONES PARA LA TELEVISIÓN POR REDES IP	
Aspectos generales	H.700–H.719
Dispositivos terminales para la televisión por redes IP	H.720–H.729
Soportes intermedios para la televisión por redes IP	H.730–H.739
Tratamiento de eventos en las aplicaciones de televisión por redes IP	H.740–H.749
Metadatos para la televisión por redes IP	H.750–H.759
Marcos de las aplicaciones multimedios para la televisión por redes IP	H.760–H.769
Exploración de los servicios hasta el punto del consumo en la televisión por redes IP	H.770–H.779
Señalización digital	H.780–H.789
SERVICIOS Y APLICACIONES MULTIMEDIOS DE CIBERSALUD	
Sistemas de salud personal	H.810–H.819
Realización de pruebas de conformidad para el interfuncionamiento de los sistemas de salud personales (HRN, PAN, LAN y WAN)	H.820–H.849
Servicios multimedios de intercambios de datos de cibersalud	H.860–H.869
Escucha segura	H.870–H.879

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

Recomendación UIT-T H.551

Arquitectura de sistemas multimedios en vehículos

Resumen

En la Recomendación UIT-T H.551 se define la configuración de los sistemas multimedios para vehículos (VMS), el modelo de referencia de la arquitectura VMS y la solución de referencia para aplicaciones multimedios VMS. También se describen aspectos de seguridad y de protección de información de identificación personal y privacidad en relación con los VMS.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T H.551	28-01-2022	16	11.1002/1000/14811

Palabras clave

Arquitectura, sistemas multimedios en vehículos.

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación UIT-T H.551

Arquitectura de sistemas multimedios en vehículos

1 Alcance

En la presente Recomendación se definen las características y la configuración de los sistemas multimedios para vehículos (VMS) y el modelo de referencia de la arquitectura de los VMS. También se establecen el modelo de referencia de la plataforma de servicios multimedios para vehículos, la pila del protocolo de referencia de transmisión convergente y el modelo de receptor de referencia de dispositivos a bordo de vehículos para aplicaciones multimedios VMS. Por último, se describen aspectos de seguridad y de protección de información de identificación personal y privacidad en relación con los VMS.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta 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 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 F.749.3] Recomendación UIT-T F.749.3 (2020), *Casos de uso y requisitos de las redes multimedios en vehículos*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 redes multimedios para vehículos (VMN) [UIT-T F.749.3]: Las VMN están integradas por la plataforma de servicios multimedios para vehículos (VMSP), redes de radiodifusión y comunicaciones, y el sistema multimedios para vehículos (VMS) en el vehículo.

3.1.2 plataforma de servicios multimedios para vehículos (VMSP) [UIT-T F.749.3]: Plataforma en la nube que facilita la prestación de servicios multimedios a los usuarios finales en vehículos.

3.1.3 sistema multimedios para vehículos (VMS) [UIT-T F.749.3]: Sistema integrado por las entradas del sistema multimedios del vehículo (VM I/P), la unidad multimedios del vehículo (VMU) y las salidas del sistema multimedios del vehículo (VM O/P).

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 función principal del VMS: Función que procesa los datos físicos, funcionales y lógicos del VMS.

3.2.2 función asociada al VMS: Función que únicamente recibe y presenta datos funcionales y lógicos de otros sistemas o subsistemas.

3.2.3 función compartida del VMS: Función que utilizan otros sistemas o subsistemas para compartir datos físicos, funcionales y lógicos e información de control.

4 Abreviaturas y acrónimos

En la presente Recomendación se definen las abreviaturas y los acrónimos siguientes:

ADAS Sistema avanzado de asistencia al conducto (*advanced driver assistance system*)

AM Modulación en amplitud (*amplitude modulation*)

ANC Supresión activa del ruido (*active noise cancellation*)

APP Aplicación (*application*)

AR Realidad aumentada (*augmented reality*)

AVM Control de visión periférica (*around view monitoring*)

bCall Llamada por avería (*breakdown call*)

BGS Exploración de fondo (*background scan*)

CA Acceso condicional (*conditional access*)

CDN Red de distribución de contenidos (*content delivery network*)

CDR Radiocomunicación digital convergente (*convergent digital radio*)

DAB Radiodifusión sonora digital (*digital audio broadcasting*)

DASH Transmisión de flujo adaptable dinámica por HTTP (*dynamic adaptive streaming over HTTP*)

DMS Sistema de supervisión del conductor (*driver monitoring system*)

DNT Interrupción del seguimiento (*do not track*)

DRM Gestión de derechos digitales (*digital rights management*)

eCall Llamada de emergencia (*emergency call*)

ECM Mensaje control de autorización (*entitlement control message*)

ECU Unidad de control electrónico (*electronic control unit*)

EMM Mensaje gestión de autorización (*entitlement management message*)

FM Modulación en frecuencia (*frequency modulation*)

GDPR Reglamento general de protección de datos (*general data protection regulation*)

HEO Órbita terrestre a gran altura (*high earth orbit*)

HLS Transmisión de flujo en directo por HTTP (*HTTP live streaming*)

HMI Interfaz hombre-máquina (*human-machine interface*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

HVAC Calefacción, ventilación y aire acondicionado (*heating, ventilation and air conditioning*)

IAM Gestión de identidad y acceso (*identity and access management*)

IBOC En la banda y en el mismo canal (*in-band on-channel*)

iCall Llamada de información (*information call*)

IP Protocolo Internet (*Internet protocol*)

LCD Pantalla de cristal líquido (*liquid crystal display*)

LED Diodo emisor de luz (*light emitting diode*)

LEO Órbita terrestre baja (*low earth orbit*)

MR Realidad mixta (*mixed reality*)

NAT Conversión de dirección de red (*network address translation*)

OBD Diagnóstico a bordo (*on-board diagnostics*)

OEM Fabricante de equipo original (*original equipment manufacturer*)

OLED Diodo orgánico emisor de luz (*organic light emitting diode*)

OS Sistema operativo (*operating system*)

OTA Por vía aérea (*over the air*)

PD Diversidad de fase (*phase diversity*)

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

PUF Función física no reproducible (*physical unclonable function*)

RDS Sistema de radiocomunicaciones de datos (*radio data system*)

RF Radiofrecuencia (*radio frequency*)

RVC Cámara de visión posterior (*rear view camera*)

TCP Protocolo de control de transferencia (*transfer control protocol*)

TMC Canal de mensajes de tráfico (*traffic message channel*)

TCU Unidad de control telemático (*telematic control unit*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

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

V2P Vehículo a persona (*vehicle-to-person*)

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

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

VM Multimedios para vehículos (*vehicular multimedia*)

VM I/P Entradas del sistema multimedios para vehículos (*vehicle multimedia system inputs*)

VM O/P Salidas del sistema multimedios para vehículos (*vehicle multimedia system outputs*)

VMN Red multimedios para vehículos (*vehicular multimedia network*)

VMS Sistema multimedios para vehículos (*vehicle multimedia system*)

VMSP Plataforma de servicios multimedios para vehículos (*vehicular multimedia service platform*)

VMU Unidad multimedios para vehículos (*vehicle multimedia unit*)

VR Realidad virtual (*virtual reality*)

5 Convenios

En la presente Recomendación:

– La expresión "es obligatorio" indica un requisito que debe cumplirse estrictamente sin variación alguna para poder alegar la conformidad con la presente Recomendación.

– La expresión "se prohíbe" indica un requisito que debe cumplirse estrictamente sin variación alguna para poder alegar la conformidad con la presente Recomendación.

– La expresión "se recomienda" indica un requisito recomendado, es decir, que no es absolutamente obligatorio y que, por consiguiente, no es indispensable para alegar la conformidad con la presente Recomendación.

– La expresión "no se recomienda" indica un requisito que no se recomienda pero que tampoco está absolutamente prohibido y que, por lo tanto, puede alegarse la conformidad con la presente Recomendación aun cuando exista.

6 Antecedentes

En la presente Recomendación se definen las características y la configuración de los sistemas multimedios para vehículos (VMS) y el modelo de referencia de la arquitectura de los VMS, de conformidad con los requisitos que figuran en [UIT-T F.749.3]. También se establecen el modelo de referencia de la plataforma de servicios multimedios para vehículos (VMSP), la pila del protocolo de referencia de transmisión convergente y el modelo de receptor de referencia de dispositivos a bordo de vehículos para aplicaciones multimedios VMS. Por último, se describen aspectos de seguridad y de protección de información de identificación personal y privacidad en relación con los VMS.

La Recomendación se estructura de la forma siguiente:

En la cláusula 7 se definen las características y la configuración de los VMS. En la cláusula 8 se establece el modelo de referencia de la arquitectura de los VMS. En la cláusula 9 se describe el modelo de referencia de la VMSP, la pila del protocolo de referencia de transmisión convergente de contenido multimedios a través de redes heterogéneas, y el modelo de receptor de referencia para dispositivos a bordo de vehículos. En la cláusula 10 se abordan aspectos de seguridad de los VMS. Y, por último, en la cláusula 11, se analizan aspectos de protección de PII y de privacidad.

7 Características y configuración de los VMS

7.1 Características de los VMS

Las características de los VMS se determinan sobre la base de los principios siguientes:

– Experiencia del usuario y funciones y aplicaciones de entretenimiento e información para el conductor y los pasajeros.

– Requisitos específicos de mercado y a escalas regional y nacional.

– Requisitos jurídicos y de obligado cumplimiento.

No obstante, las características de los VMS no abarcan la arquitectura de red general para vehículos ni la integración de varios dominios en los vehículos.

7.2 Configuración de los VMS

La configuración de los VMS se basa en los siguientes principios:

– La configuración de los VMS define los requisitos específicos de las funciones de entretenimiento y presentación de información al conductor y a los pasajeros.

– Se recomienda definir la configuración de los VMS con respecto a sus características y funciones.

– Se recomienda que la configuración de los VMS abarque los componentes físicos de dichos VMS.

– Es posible realizar varias configuraciones de los VMS.

– Se recomienda que la configuración de los VMS sea muy variable. También conviene tener en cuenta tanto los productos de VMS fabricados por los OEM como los productos adaptables comerciales para VMS.

No obstante, la configuración de los VMS no abarca la arquitectura de red general para vehículos ni la integración de varios dominios en los vehículos.

7.2.1 Factores determinantes

La configuración de los VMS se determina sobre la base de los factores enumerados a continuación:

– Requisitos de uso.

– Características y requisitos funcionales.

– Necesidades de interfaz.
– Requisitos en materia de costos.
– Requisitos de referencia.

7.3 Lista de características de los VMS

En el Cuadro 1 se enumeran las características de referencia de los VMS.

Cuadro 1 – Características de referencia de los VMS

Características	Características secundarias	Configuración
Interfaz hombre-máquina (HMI)	Tecnología de presentación	Diodo emisor de luz (LED)/Pantalla de cristal líquido (LCD)/Diodo orgánico emisor de luz (OLED), etc.
	Número de pantallas	Varias (frontal, central, posterior, etc.)
	Control	Controles habituales: botones/mandos giratorios/controles táctiles, etc.
		Controles inteligentes: Control vocal, reconocimiento facial, biometría vocal, detección de gestos, personalización, control del movimiento ocular, actuadores de información táctiles flexibles, etc.
	Interacción a través de varias pantallas	Mensajes de información emergentes en diferentes pantallas
		Presentación sincronizada o no sincronizada de archivos de vídeo
		Doble pantalla de navegación
		Elección de la interfaz de pantalla
	Lenguaje del sistema	Interfaz de usuario: requisitos lingüísticos de índole variada según la normativa en vigor
	Pantalla de la cámara	Cámara de visión posterior (RVC)/Control de visión periférica (AVM)
	Control y visualización	Pantalla y controles de calefacción, ventilación y aire acondicionado (HVAC)
		Control y pantallas de asistencia al conductor
Radiodifusión	Terrenal	Analógica: radiodifusión mediante modulación en amplitud (AM), radiodifusión mediante modulación en frecuencia (FM), radiodifusión en FM con doble sintonizador y variación de fase (PD), radiodifusión en FM con exploración de fondo (BGS), sistema de radiocomunicaciones de datos (RDS), etc.
		Digital: Radiodifusión sonora digital (DAB), radiodifusión de televisión digital terrenal (DTTD), tecnologías en la banda y en el mismo canal (IBOC), radiocomunicación digital convergente (CDR), etc.
	Por satélite	Servicios de transmisión sonora y de vídeo por satélite (por ejemplo, servicios de transmisión ininterrumpida de flujos de audio y vídeo por satélite)

Cuadro 1 – Características de referencia de los VMS

Características	Características secundarias	Configuración
Conectividad de red externa	Redes celulares	3G/4G/5G
	Satélites bidireccionales	Redes de comunicación bidireccional por satélite en órbita terrestre baja (LEO)
		Redes de comunicación bidireccional por satélite en órbita terrestre a gran altura (HEO)
	Vehículo a su entorno (V2X)	Vehículo a vehículo (V2V), Vehículo a infraestructura (V2I), Vehículo a persona (V2P)
	Redes de área local inalámbricas	Puntos de acceso IEEE 802.11
Conectividad móvil en el vehículo		Llamadas mediante sistemas "manos libres" y reproducción de música mediante redes de área personal
		Navegación por Internet mediante redes de área local IEEE 802.11
		Compartición de pantalla mediante redes de comunicación de corto alcance
		Aplicaciones de terceros de interfaz con vehículos
Configuraciones telemáticas	A distancia	Vigilancia, control y transferencia de datos del vehículo a distancia
	Llamadas	Llamadas de emergencia (eCall), llamadas de avería (bCall), llamadas de información (iCall)
Tiendas/ Programas de aplicaciones en línea	Tienda de aplicaciones	Descarga de nuevas funciones
	Compra de aplicaciones temáticas	Sustitución de presentaciones temáticas
Puesta al día por vía aérea (OTA)		Soportes lógicos OTA
Medios	Audio	Normal y de alta fidelidad
	Imagen	Formatos de índole diversa
	Vídeo	Vídeo normal con resolución diversa, realidad aumentada (AR), realidad virtual (VR), realidad mixta (MR)
Navegación	Navegación local	
	Navegación en la nube	Datos a través de módem-dispositivo telemático (3G/4G/5G) / datos móviles del usuario
	Tráfico en tiempo real	Canal de mensajes de tráfico (TMC), Grupo de expertos en protocolo de transporte (TPEG), centro de tráfico en tiempo real, etc.
	Servicios	Servicios de navegación, servicios de previsión meteorológica en tiempo real, etc.
	Funciones avanzadas	Aplicaciones inteligentes para viajes, en particular calendarios, planificadores, etc.
		Comprensión del lenguaje natural

Cuadro 1 – Características de referencia de los VMS

Características	Características secundarias	Configuración
Reconocimiento y síntesis de voz (VR)	VR local, en la nube y síntesis vocal	Reconocimiento automático del habla
		Texto a voz
Audio	Calidad de audio	Ajuste del volumen de la función de velocidad
		Algoritmos de sonido
		Supresión activa del ruido (ANC)
		Ajustes de personalización (pautas de sonido y reconocimiento facial)
		Ajuste de la posición de escucha idónea
		Tecnología de reducción de la calidad del sonido
	Configuración de los amplificadores	Amplificadores integrados de varios canales
		Amplificadores con altavoces
	Configuración del sonido	Configuración de varios altavoces: altavoces de altas frecuencias (agudos)/bajas frecuencias (bajos)/de gama completa
Seguridad		Gestión de identidad y de acceso, autenticación, autorización y auditoría de transacciones
		Seguridad de red
		Seguridad operacional
		Seguridad de aplicaciones
		Seguridad de soportes lógicos OTA
		Seguridad de soportes físicos
		Seguridad criptográfica
Privacidad		Aspectos generales de protección de datos
		Protección de información personal
		Protección de la visibilidad de los datos
		Confidencialidad, integridad y disponibilidad
Funciones inteligentes	Sistema de supervisión del conductor (DMS)	Fatiga, expresión y reconocimiento de emociones
	Salud	Controlador del ritmo cardíaco, tensiómetro
	Entorno ofimático	Aplicaciones de correo electrónico, llamadas de videoconferencia, proyección holográfica, reconocimiento de gestos, control del movimiento ocular, notas manuscritas
	Juegos	Juegos de preguntas interactivos vocales, juegos de interacción holográfica, juegos de aventura
	Aplicaciones sociales	Aplicaciones sociales en el vehículo

NOTA – Las características de seguridad y privacidad son esenciales para los VMS con configuraciones M1 a M5, pero son configurables para los VMS con configuración M0. En el Apéndice I de [UIT-T F.749.3] se dan ejemplos de VMS con configuración M0 a M5.

8 Arquitectura de los VMS

En la presente cláusula se clasifican las funciones de los VMS, así como los factores determinantes y el modelo de referencia de la arquitectura de los VMS.

8.1 Funciones de los VMS

Por lo general, las funciones de los VMS se pueden clasificar en tres categorías, a saber, funciones principales, funciones conexas y funciones compartidas.

Las funciones principales de los VMS permiten procesar datos físicos, funcionales y lógicos de los VMS. Entre esas funciones principales cabe destacar las de sintonización, procesamiento de medios y presentación.

Las funciones conexas de los VMS tienen por objeto recibir y presentar datos funcionales y lógicos de otros sistemas o subsistemas. Entre dichas funciones conexas cabe destacar las de suministro de datos de la cámara posterior del vehículo y presentación de información de llamadas de emergencia a raíz de un accidente.

Las funciones compartidas de los VMS las utilizan otros sistemas o subsistemas para compartir datos físicos, funcionales y lógicos, así como información de control. Entre dichas funciones compartidas cabe destacar la de control de climatización a través de la unidad multimedios para vehículos (VMU).

8.2 Factores determinantes de la arquitectura de los VMS

A continuación, se enumeran los factores determinantes de la arquitectura de los VMS:

– Requisitos técnicos.
– Sistema operativo, memoria y requisitos de soportes físicos.
– Características, funciones, subsistemas, y requisitos lógicos y físicos.
– Necesidades de interfaz.
– Requisitos de costos.
– Requisitos de uso.
– Requisitos de referencia.
– Requisitos de conformidad y normalización.

8.3 Modelo de referencia de la arquitectura de los VMS

La arquitectura de los VMS se define en los niveles de interfaz, subsistemas y sistemas. En la Figura 1 se presenta un modelo de referencia de dicha arquitectura.

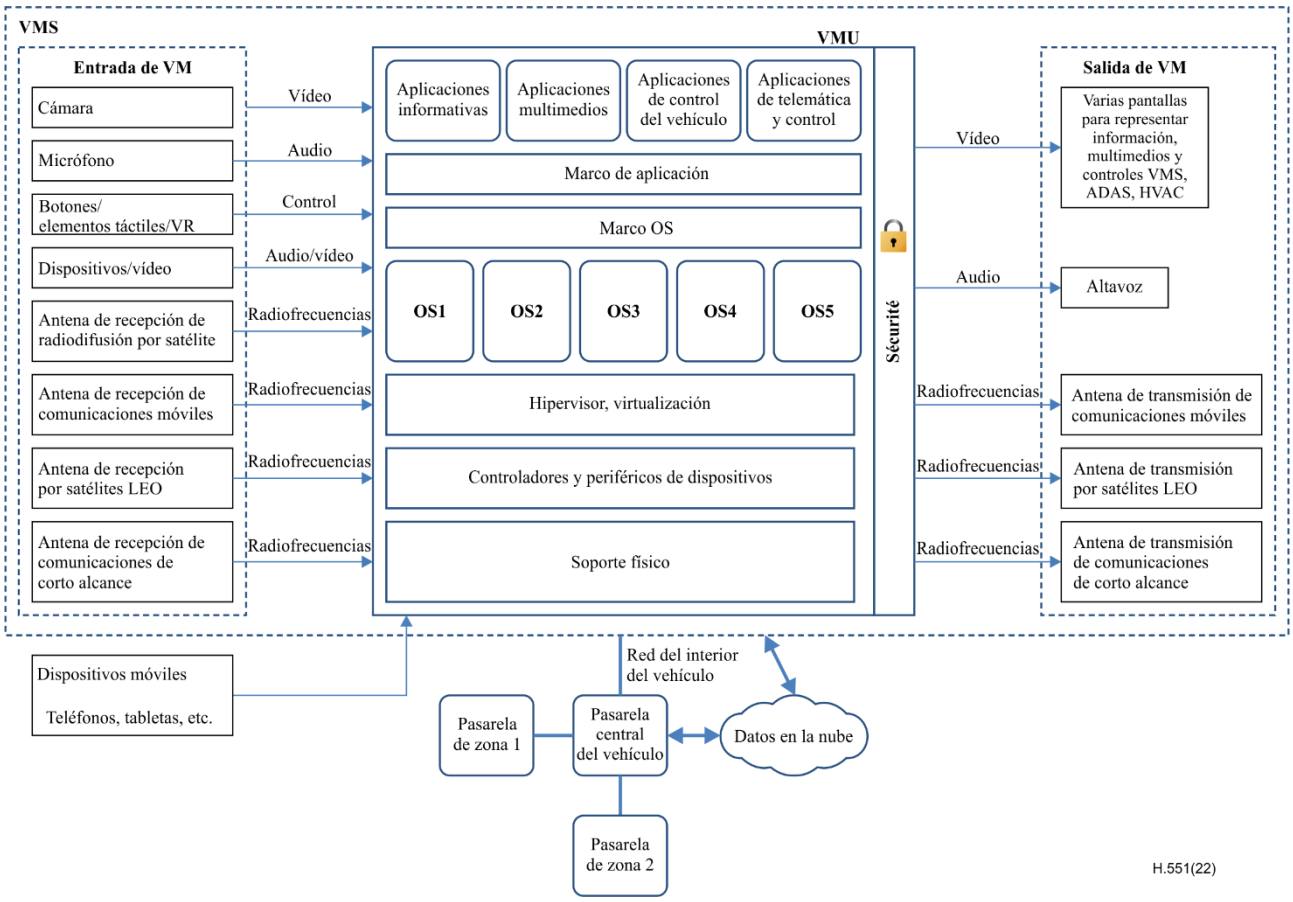

Figura 1 – Modelo de referencia de la arquitectura de los VMS

8.3.1 Aplicaciones

Entre las aplicaciones de los VMS cabe destacar:

– Aplicaciones de información, por ejemplo, cuadro de instrumentos, presentación frontal, navegación y meteorología.

– Aplicaciones multimedios, por ejemplo, medios de comunicación, navegación, VR y HMI.

– Aplicaciones de control del vehículo, por ejemplo, HVAC y conexión de vehículos.

– Aplicaciones telemáticas, por ejemplo, control remoto, diagnóstico y acceso a datos.

– Aplicaciones de presentación, por ejemplo, aplicaciones de presentación frontal y posterior.

8.3.2 Marco de aplicación

Las características y funciones de los VMS están disponibles mediante herramientas de interfaz de usuario diseñadas con arreglo a un marco de aplicación.

8.3.3 Marco del sistema operativo (OS)

El marco del sistema operativo gestiona los servicios del sistema. Puede ser un marco específico de OEM o de desarrolladores de VMS.

8.3.4 Sistema operativo

Se utilizan varios sistemas operativos (OS) y núcleos integrados en función de las necesidades de procesamiento, velocidad y precisión.

8.3.5 Hipervisión y virtualización

Las técnicas de hipervisión y virtualización tienen por objeto soportar varios sistemas operativos y tareas de procesamiento mediante un único procesador de alta potencia, por medio de compartición de recursos de computación.

8.3.6 Controladores de dispositivos y periféricos

Entre los controladores de dispositivos cabe destacar los controladores de interfaz de red del vehículo, audio y vídeo, presentación en pantalla, protocolo entre procesadores y protocolos en procesadores.

8.3.7 Soporte físico

Entre el soporte físico cabe destacar los procesadores y la memoria, así como otros componentes.

8.3.8 Datos en la nube

Los datos de la nube abarcan:

– Los datos de servicios multimedios.

– Los datos de servicios telemáticos, en particular, servicios de diagnóstico a distancia, servicios de actualización de soportes lógicos OTA, servicios *bCall* / *iCall* y servicios de navegación.

9 Aplicaciones de multimedios para VMS

En la Figura 2 se muestra un sistema de aplicaciones multimedios para VMS, integrado por una plataforma de servicios multimedios para vehículos (VMSP) en la nube, redes heterogéneas y diversos dispositivos de vehículo. Se utiliza un esquema de transmisión convergente para aumentar la eficacia de la transmisión de contenidos multimedios a través de redes heterogéneas, en particular por medio de redes de radiodifusión por satélite y redes de comunicaciones móviles. En la presente cláusula se describe el modelo de referencia de la VMSP (cláusula 9.1), la pila del protocolo de referencia de transmisión convergente de contenido multimedios a través de redes heterogéneas (cláusula 9.2), y el modelo de receptor de referencia de dispositivos a bordo de vehículos (cláusula 9.3).

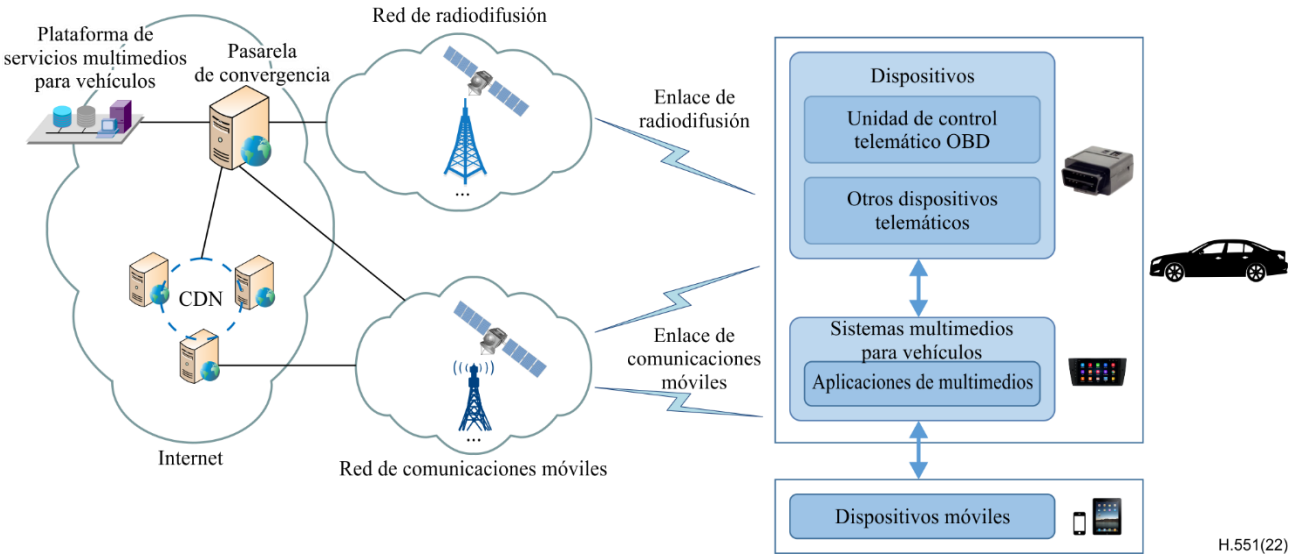

Figura 2 – Diagrama de un sistema de aplicaciones multimedios para VMS

9.1 Modelo de referencia de la VMSP

La VMSP consta de un servidor de contenido, un servidor de licencias (facultativo) y un servidor de acceso condicional (CA) (facultativo). Su modelo de referencia se ilustra en la Figura 3.

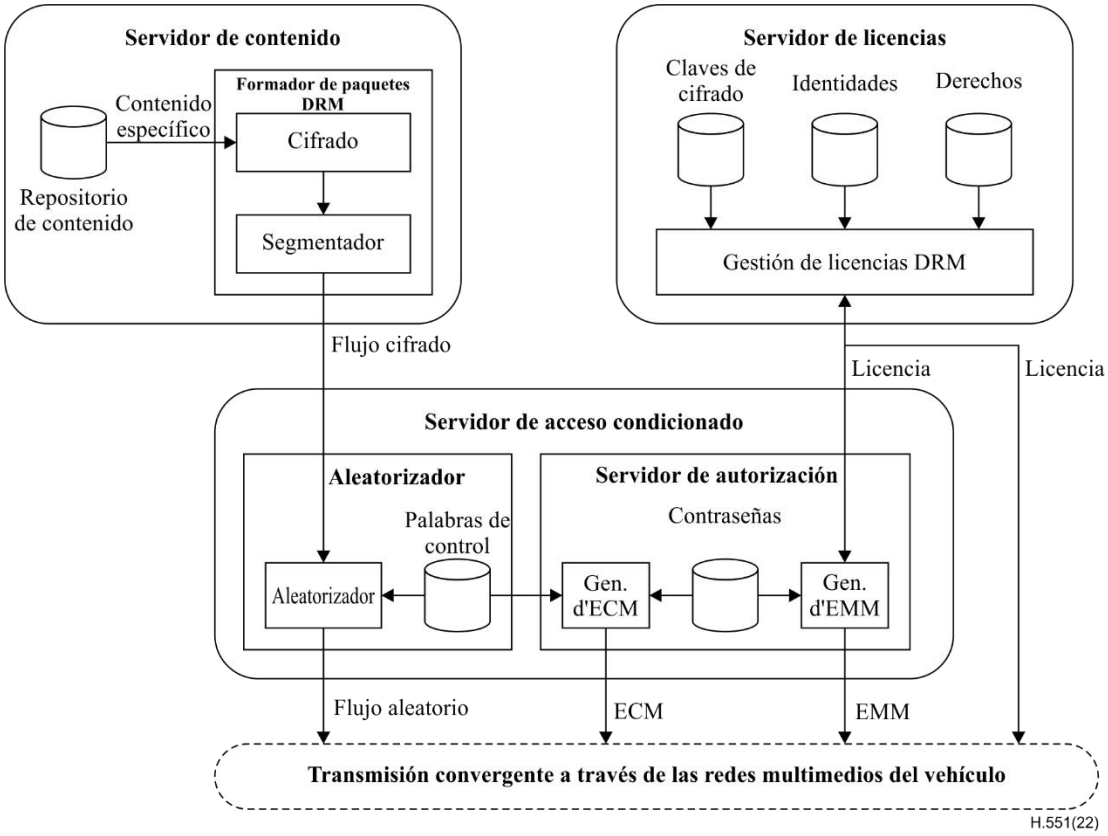

Figura 3 – Modelo de referencia de la VMSP

El servidor de contenidos está integrado por el repositorio de contenidos y el proveedor de paquetes de gestión de derechos digitales (DRM). El repositorio de contenidos tiene por objeto almacenar contenido específico que el proveedor de contenido (CP) desea distribuir. Cabe destacar que dicho repositorio de contenidos suele estar integrado en la solución DRM o, en ocasiones, en un sistema de gestión de contenidos que interactúa con el servidor DRM. El proveedor de paquetes DRM encripta el contenido multimedios y lo incluye en paquetes para su transmisión a través de la VMN. El servidor de licencias se utiliza para gestionar el establecimiento, la modificación y la revocación de licencias DRM. Éstas contienen identidades, especificación de derechos y claves de cifrado. Por lo general, los clientes DRM pueden adquirir sus licencias DRM a través del servidor de licencias mediante conexiones de redes de comunicaciones móviles. Los posibles métodos de formación de paquetes para su transmisión mediante flujos de contenido ininterrumpidos a través de VMN incluyen MPEG-DASH [b-ISO/IEC 23009-1] y HLS [b-IETF RFC 8216].

El servidor de acceso condicional (CA) está formado por un aleatorizador y un servidor de autorización. El primero se utiliza para aleatorizar la transmisión ininterrumpida de flujos de entrada mediante palabras de control. El servidor de autorización se utiliza para generar el mensaje de control de autorización (ECM) y el mensaje de gestión de derechos (EMM). Por lo general, la transmisión ininterrumpida de flujos de salida aleatorizados, ECM y EMM tiene lugar a través de redes de radiodifusión por satélite. Sin embargo, cabe distinguir las dos excepciones siguientes:

1) Cuando un usuario se desplaza a un lugar en el que no hay cobertura de telefonía móvil, las licencias DRM no pueden adquirirse a través de ninguna red de comunicaciones móviles. En ese caso, dichas licencias podrían integrarse en los EMM y transmitirse al usuario por redes de satélite. Ello facilitaría la continuidad del servicio.

2) Cuando un operador de servicio inicia su actividad, es posible que miles de nuevos clientes intenten activar sus dispositivos en un breve periodo de tiempo. Sin embargo, la anchura de banda necesaria para la transmisión de EMM para esos dispositivos puede no estar disponible en las redes de difusión por satélite. En tal caso, los EMM podrían descargarse temporalmente de las redes de radiodifusión por satélite a las redes de comunicaciones móviles. Ello permitirá garantizar una puesta en marcha satisfactoria en el plano comercial.

9.2 Pila del protocolo de referencia de transmisión convergente

Por lo general, la radiodifusión se considera el método más rentable de suministro de programas lineales a gran parte de la población de vastas zonas geográficas. Pese a la eficacia de la radiodifusión fija de TVD en las bandas Ka y Ku en todo el mundo, la prestación de servicios a vehículos mediante radiodifusión sigue constituyendo un gran reto. Por ejemplo, en entornos urbanos, la fiabilidad de las comunicaciones por radiodifusión es bastante compleja debido al desplazamiento de los receptores y al frecuente bloqueo de señal por edificios elevados. Aunque el problema de la cobertura urbana de los sistemas de radiodifusión pueda resolverse mediante la instalación de redes terrenas de repetidores que abarquen las zonas con deficiencia de servicio, la puesta en marcha de esa infraestructura de apoyo es costosa y requiere mucho tiempo. Cabe destacar asimismo la limitación adicional que presentan las comunicaciones por radiodifusión de prestar únicamente servicios unidireccionales, que no permiten la prestación de servicios personalizados ni la interacción de los usuarios.

Con objeto de afrontar esos retos, se propone un método de transmisión convergente de contenidos multimedia a través de VMN, en virtud del cual la mayor parte del contenido multimedios se transmite al conjunto de los usuarios mediante redes de radiodifusión, y las redes de comunicaciones móviles se utilizan sólo para recuperar paquetes que no hayan podido transmitirse a través de dichas redes de radiodifusión. La transmisión ininterrumpida de flujos aleatorizados de la VMSP prosigue a través de las pasarelas convergentes, en las que los segmentos multimedios se agrupan en nuevos paquetes secuenciados y se difunden a todos los usuarios a través de la red de satélites. En el terminal, los paquetes perdidos o erróneos de la transmisión de flujos ininterrumpidos de radiodifusión pueden detectarse fácilmente. Dichos paquetes se recuperan mediante su retransmisión a través de las redes de comunicaciones móviles. Una vez que la transmisión ininterrumpida de flujos de medios se vuelve a establecer sin fisuras, el terminal puede reproducirlos en las pantallas y los altavoces del cuadro de mandos, al tiempo que se utiliza como centro de entretenimiento e información local que puede compartirse por redes Wi-Fi con todos los pasajeros a través de los dispositivos personales de éstos, en particular, teléfonos inteligentes y tabletas. El citado método de transmisión convergente se ilustra en la Figura 4.

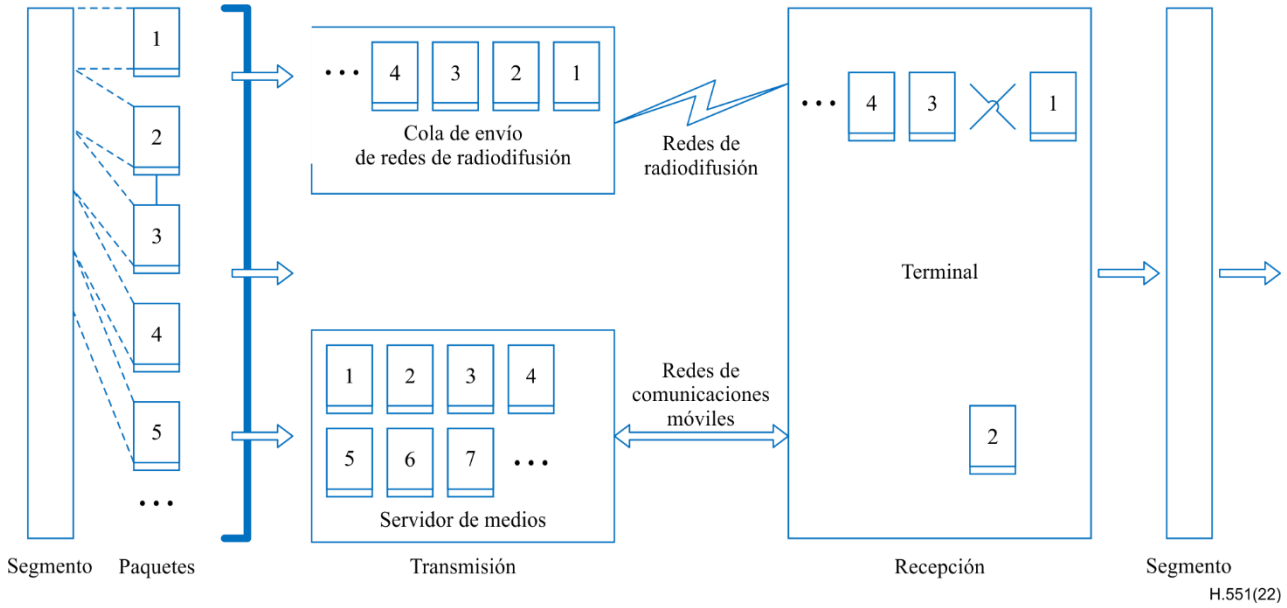

Figure 4 – Procesamiento de la transmisión convergente

El método de transmisión convergente conjuga de forma idónea las ventajas suplementarias de las redes de radiodifusión y las redes de comunicaciones móviles. De este modo, se optimiza la eficacia del sistema de prestación de servicios de transmisión ininterrumpida de multimedios a través de VMN.

La pila del protocolo de referencia de transmisión convergente de contenidos multimedios a través de VMN se muestra en la Figura 5. Cabe observar que los protocolos de transmisión convergente no dependen de las normas relativas a la capa física subyacente ni de las normas de la capa superior. En consecuencia, sólo es necesario modificar levemente las infraestructuras de comunicaciones móviles o de radiodifusión existentes.

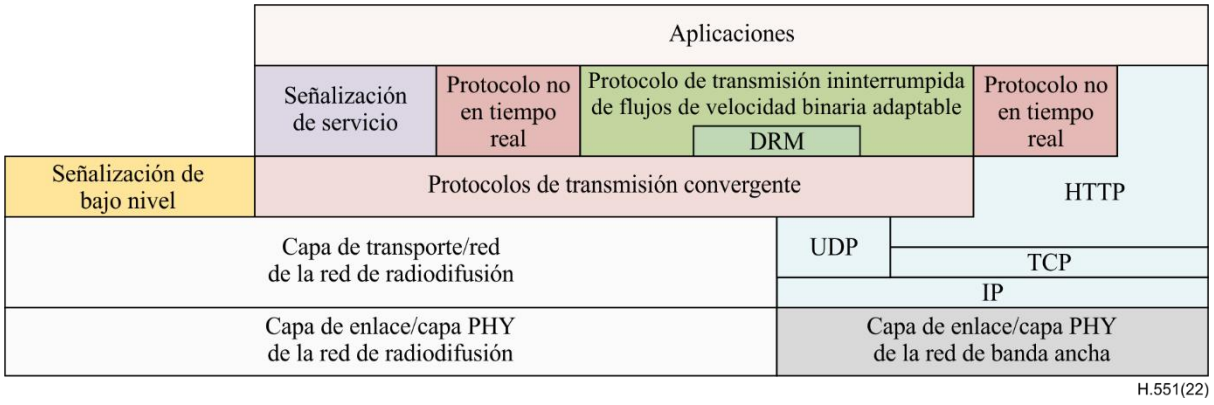

Figura 5 – Pila del protocolo de referencia de transmisión convergente

Se realiza la hipótesis general es que el protocolo de la capa de red puede basarse en ambas versiones del protocolo IP (IPv4 e IPv6). Conviene seleccionar la versión IPv6 [b-IETF RFC 8200] para garantizar una conectividad de forma directa y segura entre el VMS y las plataformas en la nube, por las razones siguientes:

– El IETF aconseja claramente a otras organizaciones de normalización (SDO) la versión IPv6 [b-IAB]. En consecuencia, se recomienda que los trabajos de normalización se basen en dicha versión IPv6.

– El espacio de direcciones IPv4 se agotó oficialmente en enero de 2011, al asignar la Autoridad de Asignación de Números de Internet (IANA) su último espacio de direcciones de nivel superior IPv4 (/8). En consecuencia, la adopción de IPv6 como único protocolo de red constituye la única solución viable para garantizar la evolución de los servicios y las aplicaciones de red.

– La transición a IPv6 sólo la consideran una iniciativa estratégica varios organismos gubernamentales. Un ejemplo, entre otros, lo representa [b-USG OMB], habida cuenta de los plazos y objetivos específicos que plantea el Gobierno Federal de los Estados Unidos para migrar las redes de las Agencias Nacionales a IPv6.

– Los dispositivos de usuario ubicados en vehículos pueden requerir accesibilidad de extremo a extremo, en particular, para conectarse a cualquier aplicación o plataforma. Este es el caso en el que no se puede conjugar la conversión de direcciones de red (NAT) [b-IETF RFC 2663] con el direccionamiento IPv4 privado. Por otro lado, IPv6 facilita plenamente un método de direccionamiento mundial que permite localizar en todo momento los dispositivos de usuario.

Pese a la mayor familiarización de la población con el protocolo IPv4, y los nuevos retos que plantea el despliegue del protocolo IPv6, el aumento de la cantidad de usuarios y tráfico de IPv6 es mucho más rápido que el de IPv4. Ello pone de manifiesto que, habida cuenta de todos los factores pertinentes, el sector industrial ha mostrado ya su preferencia por IPv6 para la utilización de [b-ETSI WP35] en el futuro.

9.3 Modelo de receptor de referencia

En la Figura 6 se muestra el modelo de receptor de referencia para dispositivos a bordo de vehículos, en el que cabe identificar las funciones siguientes:

– Conexiones de radiodifusión y de banda ancha para proporcionar al receptor la conectividad necesaria a los efectos de recepción de señales de señalización y de datos.

– Pila del protocolo de transmisión convergente/UDP/HTTP/TCP/IP y pila HTTP/TCP/IP que proporcionan protocolos de transporte orientados a objetos para que el receptor reciba recursos de la transmisión ininterrumpida de flujos de velocidad binaria adaptable (en particular, DASH o HLS) para servicios de dicha transmisión.

– Señalización de bajo nivel, transmitida a través de redes de radiodifusión que permiten al receptor elaborar una lista de servicios básicos y facilitar la detección de la señalización de servicio para cada servicio multimedios.

– Señalización de servicio, relacionada con servicios, que permite al receptor detectar servicios de transmisión ininterrumpida de flujos de multimedios y acceder a los mismos, incluidos sus componentes de contenido.

– Memoria temporal, a los efectos de almacenamiento y procesamiento de información con carácter provisional, segmentos de inicialización y segmentos de medios cuya recepción facilita la señalización del servicio.

– Servidor de transmisión ininterrumpida de flujos de velocidad binaria adaptable (DASH/HLS) a escala local, destinado a sintetizar la información de las capas subyacentes con respecto al cliente de esa transmisión ininterrumpida de flujos. Para ese cliente, la información, los segmentos de inicialización y los segmentos de medios se proporcionan a través del servidor de transmisión ininterrumpida de flujos de velocidad binaria adaptable.

– Cliente de transmisión de flujos ininterrumpida de velocidad binaria adaptable, función que procesa información y segmentos, y establece una comunicación con otros componentes del receptor para personalizar los servicios multimedios con arreglo a las capacidades de la plataforma, las preferencias del usuario y la interacción del mismo.

– Aplicación, instalada previamente o descargada, que utiliza datos transmitidos mediante radiodifusión o banda ancha con objeto de facilitar una presentación eficaz e interactiva al usuario final.

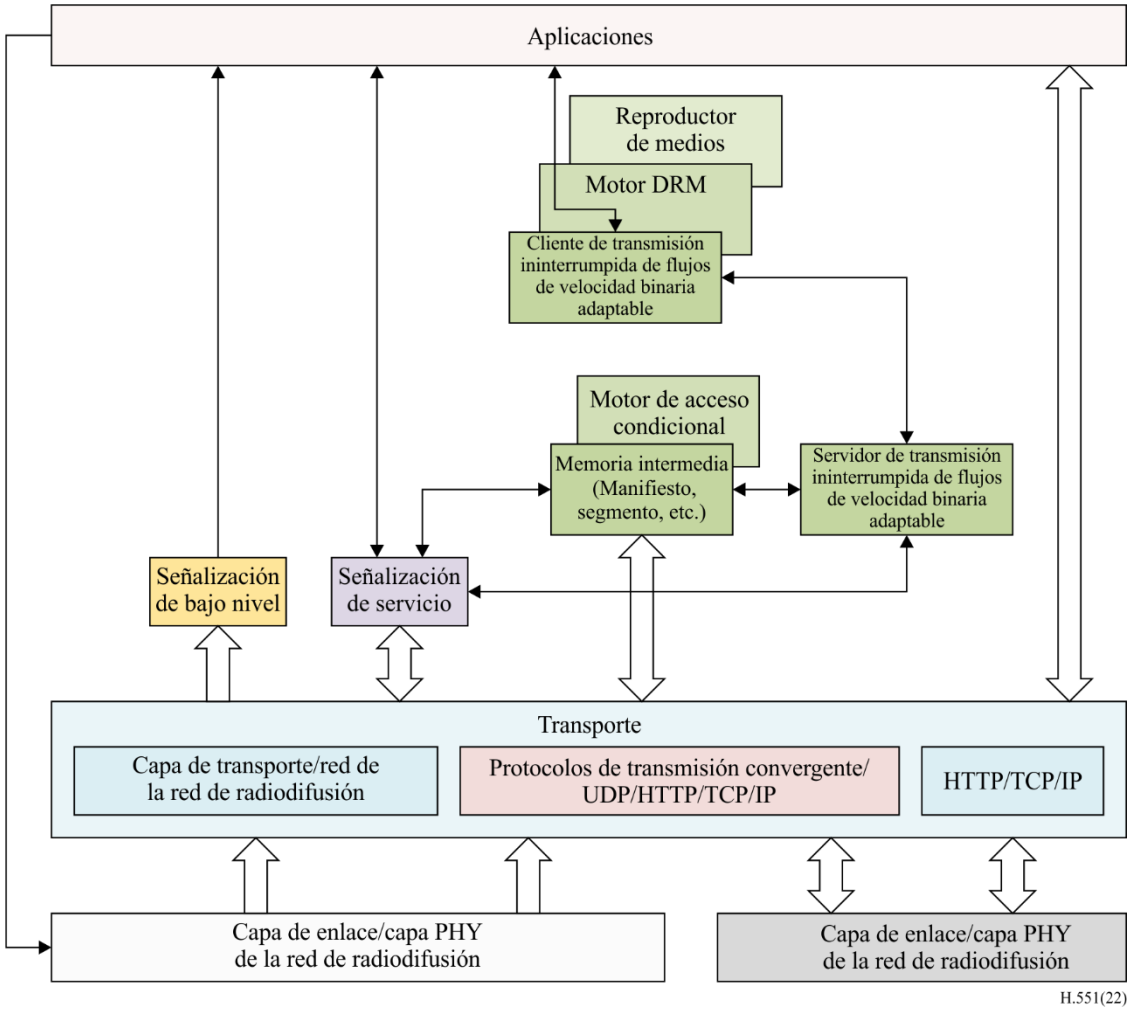

Figura 6 – Modelo de receptor de referencia de dispositivos a bordo de vehículos

A continuación se presenta una secuencia habitual de inicialización del receptor de referencia:

– La aplicación solicita una lista de servicios preconfigurados con señalización de bajo nivel. Dicha lista de servicios se transmite a la aplicación, que posteriormente facilita una interfaz de usuario para la selección de servicios de transmisión ininterrumpida de flujos de multimedios. El usuario elige uno de esos servicios.

– La aplicación utiliza la información relativa al lugar de entrada de la señalización del servicio que figura en la lista de servicios para que el servicio escogido proporcione información de acceso a la pila del protocolo de transmisión convergente/UDP /HTTP/TCP/IP a fin de recuperar la señalización de servicio. Ésta se transmite a la aplicación.

– Mediante la señalización de servicio, la aplicación proporciona información de acceso a la pila del protocolo de transmisión convergente/UDP/HTTP/TCP/IP para descargar los componentes multimedios con formato de la transmisión ininterrumpida de flujos de velocidad binaria adaptable del servicio seleccionado, que se envían ulteriormente a la memoria temporal para su almacenamiento, desaleatorización y reenvío al servidor de transmisión ininterrumpida de flujos de velocidad binaria adaptable.

– Tras la selección de un servicio, la aplicación activa el cliente de transmisión ininterrumpida de flujos de velocidad binaria adaptable, lo que provoca que el cliente DASH/HLS solicite y reciba segmentos de medios del servidor de transmisión ininterrumpida de flujos de velocidad binaria adaptable desde que esos segmentos de medios están disponibles, o posteriormente.
– Tras la recepción de los segmentos multimedios, la función compuesta que abarca el cliente de transmisión ininterrumpida de flujos de velocidad binaria adaptable, el motor DRM y el reproductor de multimedios decodifica los segmentos multimedios recibidos y los multimedios decodificados se devuelven a la aplicación para su reproducción.

10 Seguridad de los VMS

Se recomienda que la interacción entre los VMS y los demás componentes que intervienen en la seguridad de un vehículo (por lo general, la unidad de control electrónico (ECU)) se limiten a las funciones compartidas que figuran en la cláusula 8.1.

En el Anexo A se proporciona información pormenorizada al respecto.

11 Privacidad y protección de la información de identificación personal (IIP)

Se recomienda que los VMS proporcionen protección de extremo a extremo, habida cuenta de la conexión cada vez mayor de los vehículos y de los servicios interactivos que prestan. Es necesario proteger más datos de usuario e información relacionada con la privacidad a fin de garantizar la confidencialidad e integridad de los datos de usuario que se almacenan en los VMS, en el vehículo y en los sistemas en la nube de los VMS, así como en los servidores de soporte.

En el Anexo B se proporciona información pormenorizada al respecto.

Anexo A

Seguridad de los VMS

(Este anexo forma parte integrante de la presente Recomendación.)

A.1 Visión general

Se recomienda que la interacción entre los VMS y los demás componentes que intervienen en la seguridad de un vehículo (por lo general, la ECU) se limiten a las funciones compartidas que figuran en la cláusula 8.1. También se recomienda que los VMS no influyan adversamente en las funciones de los demás componentes que garantizan la seguridad necesaria de un automóvil, en particular en el caso de los vehículos de conducción autónoma.

En cuanto a la seguridad de los VMS, en la cláusula A.2 se resumen las posibles amenazas para los mismos y su ecosistema, y las funciones de seguridad frente a amenazas se proporcionan a título informativo en la cláusula A.3.

A.2 Posibles amenazas para el VMS y su ecosistema

A.2.1 Amenazas relativas a la plataforma de servicios multimedios para vehículos (VMSP)

En los últimos años, la diversificación de la conectividad en vehículos ha aumentado notablemente y, en particular, se ha hecho muy necesaria la conectividad con varios servidores situados en la VMSP. Con respecto a los VMS, los servidores de soporte se conocen como VMSP, incluidos los servidores proporcionados por los OEM, los servidores proporcionados por proveedores y los servidores proporcionados por servicios de TIC para dar apoyo al ecosistema del vehículo mediante el sistema de soporte a distancia. Cabe identificar las posibles amenazas con respecto a la VMSP:

– Utilización de servidores de soporte como medio de ataque a un vehículo o de extracción de datos.

– Interrupción de los servicios prestados por la VMSP.

– Pérdida o puesta en riesgo de los datos almacenados servidores de la VMSP.

A.2.2 Amenazas a los canales de comunicación de los vehículos

La comunicación del vehículo incluye comunicaciones externas a través de redes celulares, redes de satélites LEO, redes de radiodifusión y redes de corto alcance. Los canales utilizados para esas comunicaciones pueden ser objeto de ataque, en particular, usurpación de identidad, escucha clandestina o manipulación de mensajes. En relación con los canales de comunicación cabe identificar las siguientes amenazas:

– Manipulación, supresión u otro tipo de modificación de códigos o datos almacenados en el vehículo.

– Las interfaces de VM pueden utilizarse para acceder a otras infraestructuras (inteligentes) del vehículo (por ejemplo, la ECU no relacionada con los VMS).

– Uso de mensajes sospechosos o no fiables y ataques por apropiación de sesión/repetición.

– Puesto que las aplicaciones de VM pueden actualizarse por vía aérea, esos ataques pueden afectar también a los VM.

– Divulgación de información

  Véase la cláusula 9 de [UIT-T F.749.3].

– Ataques por denegación de servicio.

– Los VM pueden no tener acceso a infraestructura esencial dentro del vehículo, si bien pueden servir como pasarela para ataques.

– Acceso privilegiado por un usuario sin privilegios.

– Como las cuentas de usuario personalizadas pueden asociarse a las aplicaciones de VM, es posible un acceso sin privilegios. Dicho acceso sin privilegios a través de VM puede no proporcionar acceso directo a infraestructura esencial (por ejemplo, acceso al sistema raíz o al sistema de frenado), si bien puede servir también de paralela para acceder a la infraestructura del vehículo.

– Virus integrados en multimedios.

– Los VM inteligentes se basan en la transferencia de datos entre los VMS y una VMSP en la nube. Al acceder a ese canal de comunicación, los atacantes podrían utilizar la transferencia de mensajes o datos de la VMSP al VMS para instalar programas maliciosos.

– Mensajes con contenido malicioso

  Los VM inteligentes se basan en la transferencia de datos entre los VMS y una VMSP en la nube. Al acceder a ese canal de comunicación, los atacantes podrían alterar los mensajes o la transferencia de datos de la VMSP al VMS para acceder a los VMS o a las ECU del vehículo inteligente objeto del ataque.

A.2.3 Amenazas a vehículos a través de sus procedimientos de actualización

Existen dos maneras de actualizar los sistemas de los vehículos, a saber, mediante cable a través de un puerto de diagnóstico a bordo (OBD), o por medio de dispositivos portátiles como una tarjeta SD, o una memoria USB, o actualización inalámbrica por vía aérea (OTA). El *software* que hay que actualizar puede ser el del fabricante (*firmware*) o los datos de configuración del vehículo. La mayoría de los problemas electrónicos y los defectos de *software* pueden actualizarse y resolverse electrónicamente sin necesidad de acceso físico, por ejemplo, a través del probador OBD. Además, las actualizaciones por vía aérea (inalámbricas) permiten acortar el ciclo de actualización para reducir al mínimo la exposición a ataques por vulnerabilidades conocidas del *software*. Cabe identificar las siguientes amenazas en relación con los procedimientos de actualización:

– Uso indebido o puesta en peligro de los procedimientos de actualización.

  Con independencia de que se use la actualización por vía aérea o la actualización local/física, el procedimiento de actualización puede incluir amenazas basadas en programas de actualización del sistema de fabricación o *firmware* defectuoso.

  El *software* puede manipularse antes del proceso de actualización, aunque el proceso de actualización esté intacto. El proveedor de *software* crea o prepara su *software* para la actualización y lo entrega a los sistemas destinatarios que requieren la actualización. Por tanto, puede existir una grave amenaza de que pueda manipular y alterar el *software* antes de que se haya entregado.

  Especialmente durante el proceso de actualización, los materiales criptográficos tales como las claves y los certificados criptográficos utilizados en la actualización del *software* pueden quedar comprometidos y, en consecuencia, causar actualizaciones del *software* que no son válidas o que pueden resultar maliciosas.

– Denegación de servicio y de actualizaciones legítimas

  El ataque por denegación de servicio contra un servidor o una red de actualización para evitar la distribución de actualizaciones de software esencial y/o desbloquear funciones específicas del cliente puede ser un posible ataque en relación con el procedimiento de actualización de software. También es posible denegar actualizaciones legítimas.

A.2.4 Amenazas a vehículos en relación con su conectividad y sus conexiones externas

Para una gran variedad de servicios útiles, los vehículos pueden estar equipados con componentes de comunicación con servidores en la VMSP, y pueden comunicarse con cualquier dispositivo habilitado por los usuarios de las redes viales a través de una conexión inalámbrica. Además de los servicios útiles, hay beneficios para la seguridad como son la funcionalidad de llamada de emergencia automática y las que se apoyan en la comunicación V2X. Sin embargo, cuantos más vehículos se conectan a dispositivos exteriores para mejorar la conectividad, surgen más amenazas y vulnerabilidades, ya que se amplían las superficies de ataque por medio de interfaces adicionales.
Cabe identificar las siguientes amenazas en relación con la conectividad y las conexiones externas:

– Alteración de la conectividad de las funciones del vehículo.

  Los VMS no proporcionan acceso directo a las funciones esenciales del vehículo, si bien pueden utilizarse como pasarela para acceder a componentes críticos, por ejemplo, ECU específicas.

– *Software* de terceros instalado.

  Las aplicaciones VMS pueden tratarse de "software gestionado por terceros".

– Dispositivos conectados a interfaces externas.

  Como se indica en [UIT-T F.749.3], la conectividad puede basarse en dispositivos que lleve el usuario, como los teléfonos inteligentes.

A.3 Capacidades de seguridad basadas en amenazas identificadas

A.3.1 Gestión de identidad y acceso (IAM), autentificación, autorización y auditoría de transacciones

En los servicios de VMS intervienen varios administradores y usuarios, y esos servicios se utilizan, o se accede a los mismos, de forma interna o externa. La gestión de identidad no sólo es necesaria para proteger identidades, sino también para facilitar los procesos de gestión de acceso, autenticación, autorización y auditoría de transacciones en una infraestructura tan dinámica y abierta como la de los VMS.

La IAM requiere uno o varios modelos de confianza comunes para la autentificación de identidades, y los desarrolladores e "hipervisores", así como otros componentes del sistema, necesitan esos modelos a los efectos de autenticación de componentes del sistema, en particular, módulos software, aplicaciones o datos descargados.

La IAM contribuye a la confidencialidad, integridad y disponibilidad de servicios y recursos y, por ende, se convierte en una función esencial de los VMS. Por otra parte, la IAM permite crear un inicio de sesión único y una federación de identidades para los VMS mediante mecanismos de autentificación diferentes o distribuidos en varios dominios de seguridad.

La auditoría de transacciones protege contra el rechazo, permite el análisis forense tras un incidente de seguridad y sirve para disuadir los ataques (tanto por intrusión como internos). Además de mantener simple registro de eventos, la auditoría de transacciones exige un control activo para detectar actividades sospechosas.

A.3.2 Seguridad de las interfaces

Esta función permite proteger las interfaces con respecto a los desarrolladores de VMS y/o otros proveedores de VMSP, a través de los cuales se proponen varios tipos de VMS, así como las comunicaciones a través de esas interfaces. Entre los mecanismos disponibles para garantizar la seguridad de las interfaces cabe citar la autenticación unilateral/recíproca, la verificación de la integridad por suma de control, la encriptación de extremo a extremo y la firma digital.

A.3.3 Seguridad en la red

En el marco de los VMS, la seguridad de red permite aislar física y virtualmente la red y proteger las comunicaciones respecto de todos los participantes. También permite dividir el dominio de seguridad en la red, los controles de acceso en el límite de la red (por ejemplo, cortafuegos), la detección y prevención de intrusiones, la segregación del tráfico de red con arreglo a políticas de seguridad, y proteger la red contra ataques al entorno de red físico y virtual.

A.3.4 Seguridad operacional

Esta función garantiza la seguridad de la explotación y el mantenimiento cotidianos de los VMS y la infraestructura de VMSP.

Dicha función de capacidad de seguridad operacional comprende:

– La definición de un conjunto de políticas y actividades en materia de seguridad, en particular, la gestión de la configuración, la mejora de parches, la evaluación de la seguridad y las medidas de respuesta frente a incidentes.

– La supervisión de las medidas de seguridad de los VMSP y de su eficacia, incluido el envío de las notificaciones adecuadas a los VMS de que se trate.

En caso de que varíen las medidas de seguridad en materia de VMSP, o su eficacia, es necesario notificar a todos los VMS dependientes afectados.

Esos informes y notificaciones mantienen informados a los VMS autorizados sobre incidentes, información de auditoría y datos de configuración relativos a sus VMS.

A.3.5 Actualizaciones de *software* y *firmware*

Las actualizaciones OTA de forma segura deben ajustarse a las normas de seguridad establecidas. Se recomienda que en el proceso de actualización se tengan en cuenta factores operacionales (por ejemplo, el calendario pertinente y los procesos de cifrado y descifrado). La existencia de varios OEM y terceros en calidad de proveedores contribuye a la utilización de diversos interfaces de subsistema en los vehículos. En consecuencia, toda vulnerabilidad o riesgo cibernético en relación con esos OEM o proveedores podría facilitar un acceso ilegítimo a una actualización OTA de *software* legítima, y su posterior transmisión a través de los datos en la nube para su instalación en vehículos.

Se recomienda diseñar, aplicar y poner en funcionamiento un mecanismo de actualización del *software* y del *firmware* de los VMS (ECU y sistemas conexos).

En el desarrollo del servicio VMS, conviene diseñar e implementar como función básica el mecanismo de actualización del *software* y del *firmware* de los VMS. También se recomienda implementar un mecanismo de desinstalación del *software* y el *firmware*, para utilizarlo si falla una actualización.

A los efectos de utilización y soporte del servicio VMS, el dispositivo verifica la firma digital, los certificados de firma y la cadena de certificados de firma del paquete de actualización de *software/firmware* antes de que comience el proceso de actualización.

Se recomienda que las claves criptográficas utilizadas para actualizar la protección de integridad y la confidencialidad se gestionen de forma segura y se usen adecuadamente. Si las actualizaciones se realizan por vía aérea (OTA), se recomienda utilizar a tal efecto canales de comunicación cifrados.

Por último, conviene que las actualizaciones mediante OTA se realicen de forma plenamente satisfactoria, y si fallan, que ello se produzca de forma reversible. En el caso de una actualización fallida, se recomienda restaurar en el dispositivo la configuración más reciente adecuada conocida, sin interrumpir la conexión del dispositivo con el servidor de actualización.

A.3.6 Seguridad de las aplicaciones

En ocasiones, las funciones de seguridad anteriormente citadas tienen por objeto mejorar la seguridad de una "aplicación VMS", a menudo mediante la identificación y prevención de vulnerabilidades de seguridad en los VMS y su ecosistema. Cabe usar varias técnicas para identificar dichas vulnerabilidades de seguridad en diferentes etapas de la vida útil de las aplicaciones, en particular, durante su diseño, desarrollo, implantación, actualización y mantenimiento.

A.3.7 Gestión de incidentes

La gestión de incidentes consiste en la supervisión, predicción, alerta y respuesta en caso de incidente. Para saber si un VMS funciona según lo previsto en toda la infraestructura, es necesario realizar una supervisión continuada (por ejemplo, un análisis en tiempo real de la calidad de funcionamiento de los servidores usados en la VMSP). Así, el sistema capta el estado de la seguridad del servicio, identifica condiciones anormales y alerta en cuanto se produce una sobrecarga, brecha, discontinuidad, etc., del sistema de seguridad. Cuando se produce un incidente de seguridad, se determina el problema y se reacciona con celeridad, ya sea de manera automática o con la intervención de la persona que ejerce de administrador. Los incidentes resueltos se registran en un fichero y se analizan con el fin de descubrir patrones subyacentes para poder reaccionar proactivamente.

A.3.8 Cifrado

Esta función garantiza la confidencialidad e integridad de los datos utilizados e intercambiados en los VMS y sus ecosistemas. Se trata del método fundamental para almacenar y transmitir datos de una forma determinada, con objeto de que sólo sus destinatarios puedan leerlos y procesarlos. Esta función no sólo protege los datos del VMS frente a robos o alteraciones, sino que también puede utilizarse para la autenticación de usuarios, entre otras aplicaciones.

Como ejemplo adecuado de aplicación del cifrado, en [b-ITU-T X.1197 Amd1] se proporcionan directrices sobre la selección de primitivas de cifrado para los sistemas de IPTV, que pueden aplicarse a los flujos de multimedios de sistemas en vehículos, en la medida en que éstos tengan el mismo nivel de importancia o relevancia que los flujos de multimedios de los sistemas de IPTV no destinados a vehículos. De forma análoga, para los vehículos con conectividad 5G, en [b-ITU-T X.1811] se proporciona orientación suplementaria sobre la manera de aplicar los niveles de seguridad básicos de [b-ITU-T X.1197 Amd1], en particular con respecto a flujos de multimedios.

Por otro lado, en el caso de una solución DRM basada en codificación robusta y autentificada, destinada a facilitar que el sistema de información y entretenimiento sólo acepte contenidos legítimos con derechos de autor, dicho sistema de información y entretenimiento y el sistema de conducción asistida sólo tendrían en cuenta flujos de multimedios externos legítimos con visibilidad directa, con objeto de evitar interrupciones de tráfico.

A.3.9 Seguridad del *hardware*

Esta función tiene por objeto evitar vulnerabilidades y deficiencias de seguridad asociadas al *hardware* de los VMS, y proporcionar un entorno seguro para la implementación de *hardware*. En particular, la implantación de una gran cantidad de funciones de cifrado fundamentales a nivel de *hardware* ha pasado a ser esencial, por ejemplo, la gestión de claves de cifrado, las actividades de cifrado y descifrado y la provisión de firmas digitales y soluciones de autenticación robusta, que se utilizan ampliamente para garantizar la seguridad de los VMS. A tal efecto, es necesario diseñar y verificar de forma segura el funcionamiento del *hardware* conexo desde la fase de diseño del mismo, habida cuenta de posibles amenazas y ataques.

Por ejemplo, para garantizar la seguridad a nivel de ECU en la arquitectura de los VMS, se recomienda que cada ECU implementada se proteja mediante HSM y PUF, componentes habituales de los módulos de seguridad del *hardware.*

A.3.10 Funciones generales de seguridad

NOTA – Las siguientes funciones de seguridad son facultativas en el marco de la presente Recomendación. No obstante, dichas funciones pueden aplicarse de forma eficaz para mejorar la seguridad de los VMS.

– Evaluación y auditoría de la seguridad;

Esta función permite evaluar la seguridad de los VMS. La parte autorizada puede verificar que un VMS cumple los requisitos de seguridad pertinentes. La evaluación o auditoría de seguridad puede realizarla un VMS, la VSMP o un tercero, y la certificación de seguridad podría llevarla a cabo un tercero autorizado.

Deben aplicarse unos criterios de seguridad adecuados para garantizar la compatibilidad de los VMS y la VMSP en lo que respecta al nivel de seguridad.

– Modelo de confianza

Todo sistema en el que varios proveedores cooperan para ofrecer un servicio fiable requiere un modelo de confianza común.

Habida cuenta del carácter multipartito de los VMS, el entorno de los mismos debe incluir un modelo de confianza general. Este modelo de confianza permitirá la creación de islas y/o federaciones de entidades fiables, de modo que los elementos dispersos del sistema podrán autentificar la identidad y autorizar los derechos de otras entidades y componentes. Cada isla o federación de confianza se basará en una o varias autoridades de confianza (por ejemplo, una autoridad de certificados de infraestructura de clave pública.

– Aislamiento y protección de datos

a) Aislamiento de datos

El aislamiento de datos puede realizarse a nivel físico o lógico, en función de la granularidad de aislamiento necesaria y la instalación específica de *software* y *hardware* de los VMS.

b) Protección de datos

La protección de datos garantiza que los datos de los VMS y los correspondientes datos almacenados en la VMSP estén debidamente protegidos, de forma que sólo sea posible modificarlos, o acceder a los mismos, previa autorización de los VMS. Esa protección podría incluir algún tipo de combinación de listas de control de acceso, verificación de integridad, corrección de errores/recuperación de datos, y otros mecanismos adecuados.

Cuando una VMSP permite el cifrado del almacenamiento de datos de los VMS, la función de cifrado puede realizarse a nivel de cliente (en una aplicación del CSP) o de servidor.

– Coordinación de la seguridad

Puesto que cada VMS aplica diferentes controles de seguridad, esta función de seguridad se encarga de coordinar los mecanismos de seguridad heterogéneos para evitar deficiencias de protección.

Las partes que desempeñan diversas funciones en el ecosistema de los VMS tienen diferentes grados de control sobre los servicios y recursos físicos o virtuales, en particular el control de seguridad.

Cada parte dispondrá de varios mecanismos de seguridad, en particular, aislamiento del hipervisor e IAM.

Protección de red, etc. La coordinación de la seguridad depende de la compatibilidad y armonización de los diversos mecanismos de seguridad.

– Seguridad de la cadena de suministro

Una VMSP utiliza varios proveedores de servicio. Algunos de esos proveedores son del sector industrial, al tiempo que otros son proveedores habituales de equipos o servicios de tecnología de la información (TI), por ejemplo, fabricantes de *hardware* sin relación directa con los VMS. Esta función permite establecer una relación de confianza entre la VMSP y todos los participantes en la cadena de suministro mediante actividades de seguridad. Dichas actividades de seguridad consisten en identificar y recabar información acerca de los componentes y servicios adquiridos por la VMSP relativos a los VMS, así como en aplicar las políticas de seguridad en la cadena de suministro.

Por ejemplo, algunas actividades habituales de seguridad en una cadena de suministro en relación con una VMSP son las siguientes:

a) confirmación de información de base en relación con los participantes de la cadena de suministro;

b) validación del *hardware*, *software* y los servicios empleados por la VMSP;

c) inspección del *hardware* y *software* adquirido por la VMSP para garantizar que no haya sido alterado de forma ilícita previamente, en tránsito;

d) proporcionar mecanismos para verificar el origen del *software* de los VMS, por ejemplo, el código facilitado por un proveedor de *software*.

Esta función debe permitir seguir la evolución del sistema y sus actualizaciones.

– Entorno y procedimientos de desarrollo seguros

Esta función permite evitar deficiencias de seguridad en los VMS y sus ecosistemas durante la etapa de desarrollo. Un entorno de desarrollo abarca personas, procesos, tecnologías e instalaciones que guarden relación con el desarrollo de un sistema. Se recomienda que el desarrollador de servicios VMS evalúe los riesgos de cada actividad específica de desarrollo respecto de los VMS y establezca entornos de desarrollo seguros habida cuenta de los factores enumerados a continuación:

a) El personal que trabaja en cada entorno;

b) Metodologías de desarrollo aplicadas y procesos de tratamiento de datos y *software*;

c) Uso de productos y servicios subcontratados;

d) Entorno físico y de red, y

e) Compatibilidad con otras actividades de desarrollo u operacionales.

El desarrollador de servicios relativos a los VMS también debe establecer el entorno de desarrollo y los procedimientos conexos con objeto de mitigar riesgos. Se recomienda que los procedimientos se den a conocer a las personas que participan en las labores de desarrollo.

Anexo B

Protección de información de identificación personal (PII) y privacidad

(Este anexo forma parte integrante de la presente Recomendación.)

Se recomienda que los VMS proporcionen protección de extremo a extremo, habida cuenta de la conexión cada vez mayor de los vehículos y de los servicios interactivos que prestan. Es necesario proteger más datos de usuario e información relacionada con la privacidad a fin de garantizar la confidencialidad e integridad de los datos de usuario que se almacenan en los VMS, en el vehículo y en los sistemas en la nube de los VMS, así como en los servidores de soporte.

Según el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos, la PII es "todo tipo de información relativa a una persona que permita inferir razonablemente, por medios directos o indirectos, la identidad de esa persona" [b-NIST SP 800-79-2].

No existe una definición única del término "privacidad". Su significado depende del contexto jurídico, político, social, cultural o sociotecnológico de que se trate.

Por lo general, cabe definir la privacidad de información de la manera siguiente:

1) Una persona goza de privacidad de información si está protegida frente al acceso de terceros no autorizados a sus propios datos, y frente a la alteración o manipulación de esos datos.

La protección de información personal es uno de los aspectos que permiten garantizar la privacidad.

Los VMS pueden almacenar IIP o desempeñar la función de pasarela para acceder a IIP del propietario del vehículo, del conductor y/o de los demás ocupantes.

B.1 Fuentes de información

Los VMS abarcan varias fuentes de suministro de información, en particular:

– Sensores (detectores de movimiento y de ubicación, entre otros).
– Cámaras (personalización y reconocimiento de funciones, etc.).
– Micrófonos y sistemas de audio (útiles asimismo a los efectos de grabación o reconocimiento de voz, y biometría de la misma).
– Identificadores de los protocolos de comunicación de red, en particular, dirección IP o MAC, entre otros.
– Fuentes de multimedios, en particular memorias USB, tarjetas *Secure Digital*, discos duros externos, etc.
– Aplicaciones de terceros, pasarelas de pago y servicios, dispositivos o accesorios de índole diversa.

Los VMS almacenan y comparten información con otros sistemas del vehículo o en la nube, con arreglo a la arquitectura o requisitos regionales, legislativos y de certificación del vehículo.

B.2 Protección de la PII: aspectos generales

La información personal (en particular, datos, archivos de texto, audio, vídeo o imágenes) debe protegerse, incluido todo contenido que puedan solicitar usuarios que no sean el cliente legítimo o el usuario final (por ejemplo, sistemas en la nube, establecimientos o procesos a distancia) a través de los VMS.

Es necesario que exista un acuerdo para compartir datos personales de clientes, usuarios finales y terceros. Dicho acuerdo, o cualquier otro acuerdo pertinente que rija el uso de servicios VMS, ha de basarse en los siguientes criterios:

– Acceso personalizado con arreglo a la selección de servicios y preferencias del usuario.
– Diseño de los VMS para facilitar su uso de conformidad con los requisitos reglamentarios en materia de privacidad.
– El diseño del *software*, del *hardware* y de la red de los VMS sólo debe permitir un acceso autenticado.
– La protección de PII y la privacidad de los VMS debe garantizarse para vehículos particulares de un solo usuario, así como para vehículos compartidos con varios usuarios.

B.3 Visibilidad y transparencia de los datos

Es recomendable la aplicación de normas de seguridad conocidas y analizadas adecuadamente. También es conveniente evitar algoritmos de cifrado privados.

Es recomendable adoptar procesos bien conocidos.

Por otro lado, conviene informar a los usuarios de los datos almacenados o accesibles a través de los VMS. Puesto que la transparencia facilita la aceptación del usuario, se recomienda que la información destinada al mismo abarque el tipo de datos, la finalidad de su obtención, la identidad de las entidades que procesan los datos y la duración del almacenamiento de los mismos.

B.3.1 Privacidad por defecto

Es recomendable que los usuarios puedan controlar el límite de descarga de datos, y decidir si desean descargarlos o almacenarlos. Las estrategias de este tipo fomentan la privacidad y se ajustan mejor a los principios de privacidad por defecto. En consecuencia, se recomienda la formulación de esas estrategias de preferencia personal.

Por otro lado, conviene que los VMS identifiquen la lista de casos de utilización que cumplen los requisitos y parámetros pertinentes en materia de privacidad de datos

Las aplicaciones pueden utilizar recursos diversos para determinados casos de utilización. Por ejemplo, en el caso de los servicios de localización, pueden utilizarse sistemas *Bluetooth* o GPS, puntos de acceso Wi-Fi compartidos o la ubicación de torres de telefonía móvil para determinar la ubicación aproximada del usuario. Se recomienda que los VMS ofrezcan a los usuarios la posibilidad de desactivar determinadas funciones de seguimiento. A tal efecto, cabe proponer un control de configuración general con arreglo a políticas de privacidad que abarquen todas las aplicaciones. También puede facilitarse a los usuarios el control de acceso a datos relativos a una única aplicación. O pueden utilizarse controles de privacidad análogos a la propuesta de enfoques múltiples PRICON. Por otro lado, los VMS pueden incorporar la señal "Do Not Track" ("DNT"), utilizada en navegadores de Internet. La señal DNT es un encabezamiento HTTP que indica las preferencias del usuario en materia de seguimiento de la actividad del mismo con respecto a un servicio determinado, o de su seguimiento a través de varios sitios web.

En particular, determinadas aplicaciones o funciones de control pueden solicitar la recepción de datos de localización únicamente mientras se utiliza la aplicación, o habilitar esa función en todo momento. Los ocupantes pueden inhabilitar, en su caso, ese acceso, y se recomienda que puedan modificar su decisión en cualquier momento por medio de los ajustes pertinentes. Si ello es aplicable a un servicio explotado en la Unión Europea, en virtud de lo establecido en el Reglamento General de Protección de Datos (RGPD), el usuario debe poder tomar decisiones fundadas en materia de privacidad. Esa adopción de decisiones fundadas es posible si la persona que toma la decisión es consciente de las consecuencias que conlleva la divulgación de información (qué personas tienen acceso a determinados datos, con qué fin y en qué condiciones), o su denegación (las funciones específicas que se restringen).

Si se ha concedido acceso a una aplicación a determinados datos, incluida su utilización en segundo plano, es necesario recordar a los usuarios su aprobación y permitirles modificar la modalidad de acceso a la aplicación.

Conviene que la arquitectura de los VMS sea robusta, con objeto de evitar que las aplicaciones accedan a información a la que el usuario no ha concedido tácitamente autorización de acceso.

B.4 Precisión e integridad de los datos

Es recomendable que los VMS mantengan todas las funciones específicas relativas a los datos, en particular en materia de transmisión, descarga, comunicación y supresión.

Seguridad de extremo a extremo: protección a lo largo de toda la vida útil. Se recomienda la revisión periódica del código y la realización de rigurosas pruebas de seguridad. También es conveniente aplicar estrategias de protección en relación con la radiodifusión, las bases de datos y el receptor.

Es recomendable garantizar la seguridad del *software* para evitar la pérdida, la inexactitud, la alteración, la indisponibilidad o el uso indebido de los datos y recursos que se utilizan, gestionan y protegen.

Conviene asimismo que los usuarios puedan verificar la exactitud de la PII y la legitimidad de su tratamiento.

La integridad conlleva que la coherencia, exactitud y fiabilidad de los datos se mantengan a largo plazo. De ahí que sea recomendable evitar la modificación o supresión indebida de información. Conviene adoptar medidas adecuadas para evitar el rechazo de información y garantizar que ésta sea fidedigna.

Es recomendable que los usuarios puedan verificar, a través de los parámetros de configuración, qué aplicaciones han autorizado el acceso a determinada información, y conceder o revocar accesos en el futuro.

Por otro lado, es recomendable que el sistema operativo de los VMS restrinja la transmisión de datos entre las aplicaciones y las cuentas instaladas por una solución de gestión de datos de confianza y las instaladas por el usuario.

Los usuarios pueden solicitar la corrección, modificación o supresión de su información de identificación personal si ésta es inexacta, o si consideran que el tratamiento de la misma infringe la legislación en vigor al respecto.

Se deben implantar los sistemas, las aplicaciones y los procedimientos necesarios para proteger la información de identificación personal de los usuarios, y mitigar los riesgos de robo, alteración, pérdida o uso no autorizado de datos, y acceso ilegítimo a la misma.

Se recomienda detectar toda modificación no autorizada de la PII que figura en los VMS o en la nube, y notificarla al usuario.

B.5 Confidencialidad

La confidencialidad consiste en preservar las restricciones autorizadas de acceso a información y divulgación de la misma, incluidos los medios para proteger la privacidad y la información personal.

B.5.1 Grados de incidencia de la confidencialidad

Conviene evaluar la PII para determinar el grado de incidencia de su confidencialidad, a fin de aplicar las salvaguardias pertinentes. No se recomienda tratar del mismo modo toda la PII almacenada o generada.

Se recomienda definir los grados de repercusión de la confidencialidad bajo, mediano o elevado, en función de la facilidad de identificación, la confidencialidad de la información y la obligación de protegerla en el marco de la normativa en vigor.

B.5.2 Protección de la confidencialidad

Se recomienda que la protección de la confidencialidad se garantice mediante las medidas siguientes:

– Implantación de un mecanismo de control de acceso por medio de una contraseña para acceder a los datos de los VMS.

– Acceso multicapa a información confidencial cuya incidencia sea elevada.

– Control de acceso a varios niveles desde teléfonos móviles, ordenadores portátiles y dispositivos digitales personales.

– Cifrado de la PII antes de su transmisión. Las medidas pormenorizadas a tal efecto se describen en la cláusula A.3.8 (Cifrado).

Por otro lado, se recomienda llevar a cabo evaluaciones de riesgo antes del establecimiento de nuevos requisitos. Conviene asimismo implantar un mecanismo de análisis ininterrumpido de riesgos a fin de evaluar modificaciones de los VMS e identificar nuevos riesgos conexos.

B.6 Supresión de referencias a la identidad de los titulares de datos

La supresión de referencias a la identidad de los titulares de datos se basa en la alteración irreversible de datos clasificados a fin de velar por la protección de derechos en materia de PII.

La aplicación de ese proceso de supresión de referencias a los datos que se procesan en el entorno de los VMS facilita la realización de una amplia gama de análisis y la compartición de datos.

B.7 Disponibilidad de datos

La disponibilidad de datos conlleva la utilización de la información, y el acceso a la misma, de forma oportuna y eficaz.

Es aconsejable proporcionar a los ocupantes autorizados un control pormenorizado y prioritario, con respecto a los servicios del sistema, del uso de la información de localización. Ello incluye la posibilidad de desactivar la obtención de datos de localización en relación con la información que recopilan las aplicaciones internas, el historial de búsqueda de navegación y la información de acceso mediante Bluetooth y Wi-Fi. Si el usuario se inscribe en el sistema en la nube de un OEM, las aplicaciones necesarias en el plano funcional tendrán acceso por defecto a dicho sistema en la nube. Conviene que los usuarios controlen el acceso de cada aplicación a la nube por medio de los parámetros pertinentes.

Si se accede a PII a distancia por medio de aplicaciones telemáticas, se recomienda que los servicios establezcan su conexión y funcionen mediante autenticación de varios niveles.

Habida cuenta de la disponibilidad de datos en formato cifrado (por ejemplo, cifrado homomórfico), tras varias etapas de procesamiento (cálculo, procesamiento estadístico, etc.), se puede realizar un procesamiento de datos análogo en los VMS.

Bibliografía

[b-UIT-T X.1197 Amd1] Recomendación UIT-T X.1197 Amd.1 (2019), *Directrices sobre criterios para la selección de algoritmos criptográficos para la protección de los servicios y contenidos de TVIP, Enmienda 1*.

[b-UIT-T X.1811] Recomendación UIT-T X.1811 (2020), *Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas 5G*.

[b-ETSI WP35] ETSI White Paper 35 (2020), *IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward*. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_WP35_IPv6_Best_Practices_Benefits_Transition_Challenges_and_the_Way_Forward.pdf

[b-IEEE 802.11] IEEE 802.11-2020 – *Norma del IEEE sobre tecnología de la información – Telecomunicaciones e intercambio de información entre redes de área local y metropolitana – Requisitos específicos Parte 11: Especificaciones del control de acceso al medio (MAC) LAN inalámbrico y de la capa física (PHY).*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

[b-IETF RFC 8200] IETF RFC 8200 (julio de 2017), *Internet Protocol, Version 6 (IPv6) Specification.*

[b-IETF RFC 8216] IETF RFC 8216 (2017), *HTTP Live Streaming*.

[b-ISO/CEI 23009-1] ISO/CEI 23009-1:2019, *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*.

[b-IAB] Declaración de la Comisión de Arquitectura de Internet (IAB) sobre agotamiento de direcciones IPv6 (2016). https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ [Online].

[b-NIST SP 800-79-2] Publicación especial del NIST, 800-79-2 (2015), *Guidelines for the Authorization of Personal Identity Verification Card Issues (PCI) and Derived PIV Credential Issuers (DPCI).*

[b-USG OMB] Oficina y Gestión de Presupuesto de EE.UU. (noviembre de 2020), *Memorandum for heads of executive departments and agencies*. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf [en línea].

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 multimedios**
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, 2022