Reglamento n.º 155 de la Comisión Económica para Europa (CEPE) de las Naciones Unidas — Disposiciones uniformes relativas a la homologación de los vehículos de motor en lo que respecta a la ciberseguridad y al sistema de gestión de esta [2021/387]

Fecha de entrada en vigor: 22 de enero de 2021

El presente documento tiene valor meramente informativo. Los textos auténticos y jurídicamente vinculantes son los siguientes:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 y

— ECE/TRANS/WP.29/2020/97

ÍNDICE

REGLAMENTO

1. Ámbito de aplicación
2. Definiciones
3. Solicitud de homologación
4. Marcados
5. Homologación
6. Certificado de conformidad del sistema de gestión de la ciberseguridad
7. Especificaciones
8. Modificación del tipo de vehículo y extensión de la homologación de tipo
9. Conformidad de la producción
10. Sanciones por falta de conformidad de la producción
11. Cese definitivo de la producción
12. Nombres y direcciones de los servicios técnicos responsables de realizar los ensayos de homologación y de las autoridades de homologación de tipo

ANEXOS

1 Ficha técnica

2 Comunicación

3 Disposición de la marca de homologación

4 Modelo de certificado de conformidad del sistema de gestión de la ciberseguridad

5 Lista de amenazas y sus correspondientes medidas de mitigación

1. ÁMBITO DE APLICACIÓN

1.1. El presente Reglamento es aplicable a los vehículos de las categorías M y N, en lo que respecta a la ciberseguridad.

El presente Reglamento es aplicable también a los vehículos de la categoría O si llevan instalada al menos una unidad de control electrónico.

1.2. Asimismo, el presente Reglamento es aplicable a los vehículos de las Categorías L_6 y L_7 si están equipados con funciones de conducción automatizada desde el nivel 3 en adelante, tal y como se definen en el «Documento de referencia en el que se proponen las definiciones de la conducción automatizada en el marco del Grupo de Trabajo 29 (WP.29) y de los principios generales para la elaboración de un Reglamento de las Naciones Unidas sobre los vehículos automatizados» (ECE/TRANS/WP.29/1140).

1.3. El presente Reglamento debe entenderse sin perjuicio de otros Reglamentos de las Naciones Unidas, de la legislación regional o nacional que rige el acceso de partes autorizadas al vehículo, sus datos, funciones y recursos, así como las condiciones de dicho acceso. Se entenderá también sin perjuicio de la aplicación de la legislación nacional y regional en materia de privacidad y protección de las personas físicas con respecto al tratamiento de sus datos personales.

1.4. El presente Reglamento se entenderá sin perjuicio de otros Reglamentos de las Naciones Unidas y de la legislación nacional o regional por los que se rigen el desarrollo y la instalación o la integración de sistemas de sustitución de piezas y componentes, físicos y digitales, con respecto a la ciberseguridad.

2. DEFINICIONES

A los efectos del presente Reglamento, se entenderá por:

2.1. «Tipo de vehículo»: los vehículos que no difieran entre sí en al menos los siguientes aspectos esenciales:

a) la designación del tipo de vehículo dada por el fabricante;

b) aspectos esenciales de la arquitectura eléctrica y electrónica y las interfaces externas con respecto a la ciberseguridad;

2.2. «Ciberseguridad»: la condición en la cual los vehículos de carretera y sus funciones se encuentran protegidos de ciberamenazas a sus componentes eléctricos o electrónicos.

2.3. «Sistema de gestión de la ciberseguridad»: un enfoque sistemático basado en el riesgo, por el que se definen los procesos organizativos, las responsabilidades y la gobernanza para abordar los riesgos asociados con las ciberamenazas a los vehículos y para protegerlos de ciberataques.

2.4. «Sistema»: conjunto de componentes o subsistemas que ejecuta una función o funciones.

2.5. «Fase de desarrollo»: periodo que precede a la homologación de tipo de un tipo de vehículo.

2.6. «Fase de producción»: duración de la producción de un tipo de vehículo.

2.7. «Fase de posproducción»: período que transcurre entre el momento en que un tipo de vehículo se deja de producir y el final de la vida útil de todos los vehículos de dicho tipo. Los vehículos que incorporan un tipo de vehículo específico seguirán funcionando durante esta fase, pero dejarán de producirse. La fase concluye cuando ya no hay vehículos de un tipo de vehículo concreto en funcionamiento.

2.8. «Medida de mitigación»: una medida que contribuye a reducir los riesgos.

2.9. «Riesgo»: la posibilidad de que una determinada amenaza se aproveche de las vulnerabilidades de un vehículo y, al hacerlo, ocasione daños a la organización o a una persona.

2.10. «Evaluación de riesgos»: proceso general de detección, reconocimiento y descripción de los riesgos (identificación del riesgo) con vistas a comprender la naturaleza del riesgo y determinar su nivel (análisis del riesgo), y a comparar los resultados del análisis del riesgo con los criterios de riesgo para determinar si este y su magnitud son aceptables o tolerables (valoración de riesgos).

2.11. «Gestión del riesgo»: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

2.12. «Amenaza»: la posible causa de un incidente no deseado que pueda ocasionar daños a un sistema, una organización o una persona.

2.13. «Vulnerabilidad»: una debilidad de un elemento o de una medida de mitigación que pueda ser aprovechada por una o varias amenazas.

3. SOLICITUD DE HOMOLOGACIÓN

3.1. La solicitud de homologación de un tipo de vehículo en lo que concierne a la ciberseguridad será presentada por el fabricante del vehículo o por su representante debidamente acreditado.

3.2. Deberá ir acompañada de los documentos que se mencionan a continuación, por triplicado, así como de los elementos siguientes:

3.2.1. una descripción del tipo de vehículo en lo que concierne a los aspectos especificados en el anexo 1 del presente Reglamento.

3.2.2. En los casos en que dicha información resulte estar cubierta por derechos de propiedad industrial o esté constituida por conocimientos especializados del fabricante o sus proveedores, el fabricante o sus proveedores facilitarán información suficiente para que puedan realizarse correctamente los ensayos a que se refiere el presente Reglamento. Dicha información se tratará de forma confidencial.

3.2.3. El certificado de conformidad para sistemas de gestión de la ciberseguridad con arreglo al punto 6 del presente Reglamento.

3.3. La documentación deberá estar disponible en dos partes:

a) la documentación oficial para la homologación, que contendrá el material especificado en el anexo 1, se presentará a la autoridad de homologación o a su servicio técnico cuando se presente la solicitud de homologación de tipo. La autoridad de homologación o su servicio técnico utilizarán dicha información como la referencia básica para el proceso de homologación. La autoridad de homologación o su servicio técnico se asegurarán de que esta documentación esté disponible durante al menos diez años a partir del momento en el que se interrumpa definitivamente la producción del tipo de vehículo;

b) el material adicional pertinente para los requisitos del presente Reglamento, que podrá conservar el fabricante, pero que se presentará a inspección en el momento de la homologación de tipo. El fabricante garantizará que todo material presentado a inspección en el momento de la homologación de tipo esté disponible durante un período mínimo de diez años a partir del momento en el que se interrumpa definitivamente la producción del tipo de vehículo.

4. MARCADO

4.1. Se colocará una marca de homologación internacional, de manera visible y en un lugar fácilmente accesible especificado en el formulario de homologación, en cada vehículo que se ajuste a un tipo de vehículo homologado con arreglo al presente Reglamento; la marca consistirá en:

4.1.1. La letra mayúscula «E» dentro de un círculo seguida del número distintivo del país que ha concedido la homologación.

4.1.2. El número del presente Reglamento, seguido de la letra «R», un guion y el número de homologación a la derecha del círculo descrito en el punto 4.1.1.

4.2. Si el vehículo se ajusta a un tipo de vehículo homologado de acuerdo con uno o varios Reglamentos adjuntos al Acuerdo en el país que haya concedido la homologación con arreglo al presente Reglamento, no es necesario repetir el símbolo que se establece en el punto 4.1.1; en ese caso, el Reglamento, los números de homologación y los símbolos adicionales de todos los Reglamentos según los cuales se ha concedido la homologación en el país que la concedió de conformidad con el presente Reglamento se colocarán en columnas verticales a la derecha del símbolo exigido en el punto 4.1.1.

4.3. La marca de homologación aparecerá claramente legible y será indeleble.

4.4. La marca de homologación se situará en la placa informativa del vehículo colocada por el fabricante, o cerca de la misma.

4.5. En el anexo 3 del presente Reglamento figuran algunos ejemplos de las marcas de homologación.

5. HOMOLOGACIÓN

5.1. Las autoridades de homologación concederán, cuando proceda, la homologación de tipo en lo que concierne a la ciberseguridad únicamente a los tipos de vehículos que cumplan los requisitos previstos en el presente Reglamento.

5.1.1. La autoridad de homologación o el servicio técnico verificarán mediante el control de los documentos que el fabricante del vehículo haya adoptado las medidas necesarias con respecto al tipo de vehículo a fin de:

a) recopilar y verificar la información requerida en virtud del presente Reglamento a través de la cadena de suministro a fin de constatar que se detectan y gestionan los riesgos relacionados con los proveedores;

b) documentar la evaluación de riesgos (realizada durante la fase de desarrollo o con carácter retrospectivo), los resultados de los ensayos y las medidas de mitigación aplicadas al tipo de vehículo, incluida la información relativa al diseño que respalde la evaluación de riesgos;

c) aplicar las medidas de ciberseguridad adecuadas al diseño del tipo de vehículo;

d) detectar los posibles ataques a la ciberseguridad y responder a ellos;

e) registrar los datos para facilitar la detección de ciberataques y proporcionar capacidad forense en relación con los datos a fin de permitir el análisis de los intentos de ciberataques o de los ciberataques consumados.

5.1.2. La autoridad de homologación o el servicio técnico verificará, mediante ensayos en un vehículo del tipo de vehículo que su fabricante haya aplicado, las medidas de ciberseguridad que ha documentado. Los ensayos los realizarán la autoridad de homologación o el servicio técnico, por sí mismos o en colaboración con el fabricante del vehículo mediante un muestreo. El muestreo se centrará, entre otros, en los riesgos que se consideraron altos durante la evaluación de riesgos.

5.1.3. La autoridad de homologación o el servicio técnico denegarán la concesión de la homologación de tipo en lo que respecta a la ciberseguridad cuando el fabricante del vehículo no cumpla uno o varios de los requisitos a que se refiere el punto 7.3, en particular si:

a) el fabricante del vehículo no ha realizado la evaluación exhaustiva de riesgos a que se refiere el punto 7.3.3, incluso en caso de que el fabricante no haya considerado todos los riesgos relacionados con las amenazas a que se refiere la parte A del anexo 5;

b) el fabricante del vehículo no ha protegido el tipo de vehículo contra los riesgos detectados en la evaluación de riesgos del fabricante del vehículo o no ha aplicado las medidas de mitigación tal y como requiere el punto 7;

c) el fabricante del vehículo no ha adoptado medidas adecuadas y proporcionadas para garantizar entornos específicos del tipo de vehículo (si se incluyen) para el almacenamiento y la ejecución del *software*, los servicios, las aplicaciones o los datos posventa;

d) el fabricante del vehículo no ha realizado, antes de la homologación, ensayos adecuados y suficientes para verificar la eficacia de las medidas de seguridad aplicadas.

5.1.4. La autoridad de homologación que realiza la evaluación también denegará la concesión de la homologación de tipo en lo que respecta a la ciberseguridad cuando dicha autoridad o el servicio técnico no hayan recibido información suficiente del fabricante del vehículo para evaluar la ciberseguridad del tipo de vehículo.

5.2. La concesión, la extensión o la denegación de la homologación de un tipo de vehículo con arreglo al presente Reglamento se comunicará a las Partes contratantes en el Acuerdo de 1958 que apliquen el presente Reglamento por medio de un formulario que se ajuste al modelo que figura en su anexo 2.

5.3. Las autoridades de homologación no concederán ninguna homologación de tipo sin verificar que el fabricante haya establecido disposiciones y procedimientos satisfactorios para gestionar correctamente los aspectos de ciberseguridad contemplados en el presente Reglamento.

5.3.1. La autoridad de homologación y sus servicios técnicos se asegurarán de que, además de cumplir los criterios establecidos en el anexo 2 del Acuerdo de 1958, también cuentan con:

a) personal competente con capacidades de ciberseguridad adecuadas y conocimientos específicos sobre evaluaciones de riesgos en el ámbito de la automoción ([1]);

b) procedimientos para realizar la evaluación uniforme que se prevé en el presente Reglamento.

([1]) Por ejemplo, ISO 26262-2018, ISO/PAS 21448 e ISO/SAE 21434.

5.3.2. Cada Parte contratante que aplique el presente Reglamento notificará e informará mediante su autoridad de homologación a otras autoridades de homologación de las Partes contratantes que apliquen el presente Reglamento de Naciones Unidas sobre el método y los criterios que la autoridad de notificación ha tomado como base para evaluar la idoneidad de las medidas adoptadas de acuerdo con el presente Reglamento, en particular con los puntos 5.1, 7.2 y 7.3.

Esta información se compartirá: a) únicamente antes de conceder por primera vez una homologación de conformidad con el presente Reglamento y b) cada vez que se actualicen el método o los criterios de evaluación.

El objeto de intercambiar esta información es recoger y analizar las mejores prácticas a fin de garantizar la aplicación convergente del presente Reglamento por parte de todas las autoridades de homologación que lo apliquen.

5.3.3. La información a que se refiere el punto 5.3.2 se incorporará, en inglés, a la base de datos segura de Internet «DETA» ([2]), creada por la Comisión Económica para Europa de las Naciones Unidas, a su debido tiempo y a más tardar catorce días antes de que se conceda una homologación por primera vez con arreglo a los métodos y criterios de evaluación correspondientes. La información será suficiente para entender los niveles de rendimiento mínimos adoptados por la autoridad de homologación para cada requisito específico a que se refiere el punto 5.3.2, así como los procesos y las medidas que aplica para verificar que se cumplen dichos niveles ([3]).

5.3.4. Las autoridades de homologación que reciben la información a que se refiere el punto 5.3.2 podrán formular observaciones a la autoridad de homologación notificante, incorporándolas a la base de datos DETA en los catorce días posteriores a la notificación.

5.3.5. Si la autoridad de homologación otorgante no puede tener en cuenta las observaciones recibidas de acuerdo con el punto 5.3.4, las autoridades de homologación que hayan enviado las observaciones y la autoridad de homologación otorgante solicitarán aclaraciones adicionales de conformidad con el anexo 6 del Acuerdo de 1958. El correspondiente Grupo de trabajo auxiliar ([4]) del Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (WP.29) para el presente Reglamento acordará una interpretación común de los métodos y los criterios de evaluación ([5]). Se aplicará dicha interpretación común y todas las autoridades de homologación expedirán en consecuencia homologaciones de tipo en virtud del presente Reglamento.

5.3.6. Cada autoridad de homologación que conceda una homologación de tipo con arreglo al presente Reglamento notificará a otras autoridades de homologación la homologación concedida. La autoridad de homologación incorporará la homologación de tipo junto con la documentación complementaria, en lengua inglesa, a la base de datos DETA en un plazo de catorce días a partir de la fecha de concesión de la homologación ([6]).

5.3.7. Las Partes contratantes podrán estudiar las homologaciones concedidas sobre la base de la información incorporada con arreglo al punto 5.3.6. En caso de que haya opiniones divergentes entre las Partes contratantes, estas se resolverán de acuerdo con el artículo 10 y el anexo 6 del Acuerdo de 1958. Las Partes contratantes también informarán al correspondiente Grupo de trabajo auxiliar del Foro Mundial para la Armonización de la Reglamentación sobre Vehículos (WP.29) sobre las interpretaciones divergentes en el sentido del anexo 6 del Acuerdo de 1958. El Grupo de trabajo pertinente asistirá en la conciliación de las opiniones divergentes y podrá consultar con el WP.29 sobre este punto si fuera necesario.

5.4. A efectos del punto 7.2 del presente Reglamento, el fabricante velará por que se apliquen los aspectos de ciberseguridad contemplados en el presente Reglamento.

([2]) https://www.unece.org/trans/main/wp29/datasharing.html

([3]) Las orientaciones sobre la información detallada (p. ej., el método, los criterios y el nivel de rendimiento) que debe incorporarse, así como el formato, se facilitarán en el documento interpretativo que el Grupo de estudio sobre ciberseguridad y cuestiones de transmisión inalámbrica está elaborando para la séptima sesión del Grupo de trabajo sobre vehículos automatizados/autónomos y conectados (GRVA).

([4]) El Grupo de trabajo sobre vehículos automatizados/autónomos y conectados (GRVA).

([5]) Esta interpretación se reflejará en el documento interpretativo a que se refiere la nota a pie de página del punto 5.3.3.

([6]) El GRVA elaborará más información sobre los requisitos mínimos de documentación durante su séptima sesión.

6. CERTIFICADO DE CONFORMIDAD DEL SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD

6.1. Las Partes contratantes designarán una autoridad de homologación para que lleve a cabo la evaluación del fabricante y expida un certificado de conformidad del sistema de gestión de la ciberseguridad.

6.2. La solicitud de un certificado de conformidad del sistema de gestión de la ciberseguridad será presentada por el fabricante del vehículo o por su representante debidamente acreditado.

6.3. Dicha solicitud deberá ir acompañada de los documentos que se mencionan a continuación, por triplicado, así como de los elementos siguientes:

6.3.1. documentos que describan el sistema de gestión de la ciberseguridad;

6.3.2. una declaración firmada conforme al modelo definido en el apéndice 1 del anexo 1.

6.4. En el contexto de la evaluación, el fabricante declarará haber utilizado el modelo definido en el apéndice 1 del anexo 1, y demostrará a satisfacción de la autoridad de homologación o de su servicio técnico que cuenta con los procesos necesarios para cumplir todos los requisitos del presente Reglamento en lo que respecta a la ciberseguridad.

6.5. Cuando dicha evaluación se haya realizado de forma satisfactoria y se haya recibido una declaración firmada del fabricante conforme al modelo definido en el apéndice 1 del anexo 1, se otorgará al fabricante un certificado de conformidad del sistema de gestión de la ciberseguridad tal y como se describe en el anexo 4 del presente Reglamento.

6.6. La autoridad de homologación o su servicio técnico utilizarán el modelo establecido en el anexo 4 del presente Reglamento para el certificado de conformidad del sistema de gestión de la ciberseguridad.

6.7. El certificado de conformidad del sistema de gestión de la ciberseguridad tendrá una validez de un máximo de tres años a partir de la fecha de su expedición, a menos que sea retirado.

6.8. La autoridad de homologación que haya concedido el certificado de conformidad del sistema de gestión de la ciberseguridad podrá verificar, en cualquier momento, que se siguen cumpliendo los requisitos para su concesión. La autoridad de homologación retirará dicho certificado si dejan de cumplirse los requisitos establecidos en el presente Reglamento.

6.9. El fabricante informará a la autoridad de homologación o a su servicio técnico de cualquier modificación que afecte a la pertinencia del certificado de conformidad del sistema de gestión de la ciberseguridad. Tras consultar al fabricante, la autoridad de homologación o su servicio técnico decidirán si es necesario realizar nuevos controles.

6.10. A su debido tiempo, permitiendo a la autoridad de homologación completar su evaluación antes del fin del período de validez del certificado de conformidad del sistema de gestión de la ciberseguridad, el fabricante solicitará uno nuevo o la extensión de un certificado existente. Tras una evaluación positiva, la autoridad de homologación expedirá un nuevo certificado de conformidad del sistema de gestión de la ciberseguridad o ampliará la validez del existente durante un periodo adicional de tres años. La autoridad de homologación verificará que el sistema de gestión de la ciberseguridad sigue cumpliendo los requisitos del presente Reglamento. La autoridad de homologación expedirá un nuevo certificado cuando ella o su servicio técnico hayan tenido conocimiento de cambios y dichos cambios se hayan reevaluado de forma positiva.

6.11. El vencimiento o la retirada del certificado de conformidad del sistema de gestión de la ciberseguridad del fabricante se considerarán, en lo que respecta a los tipos de vehículos para los que es pertinente el sistema de gestión de la ciberseguridad, una modificación de la homologación a que se refiere el punto 8, que podrá incluir la retirada de la homologación si han dejado de cumplirse las condiciones para su concesión.

7. ESPECIFICACIONES

7.1. Especificaciones generales

7.1.1. Los requisitos del presente Reglamento no limitarán las disposiciones o los requisitos de otros Reglamentos de las Naciones Unidas.

7.2. Requisitos relativos al sistema de gestión de la ciberseguridad

7.2.1. Para la evaluación, la autoridad de homologación o su servicio técnico verificarán que el fabricante del vehículo cuenta con un sistema de gestión de la ciberseguridad, así como la conformidad de dicho sistema con el presente Reglamento.

7.2.2. El sistema de gestión de la ciberseguridad cubrirá los siguientes aspectos:

7.2.2.1. el fabricante del vehículo demostrará a una autoridad de homologación o servicio técnico que su sistema de gestión de la ciberseguridad se aplica a las siguientes fases:

a) la fase de desarrollo;

b) la fase de producción:

c) la fase de posproducción.

7.2.2.2. El fabricante del vehículo demostrará que los procesos utilizados en su sistema de gestión de la ciberseguridad garantizan una consideración adecuada de la seguridad, incluidos los riesgos y las medidas de mitigación enumerados en el anexo 5. Se considerarán:

a) los procesos utilizados en la organización del fabricante para gestionar la ciberseguridad;

b) los procesos utilizados para detectar los riesgos para los tipos de vehículos. Dentro de dichos procesos, se tendrán en cuenta las amenazas indicadas en la parte A del anexo 5 y otras amenazas pertinentes;

c) los procesos utilizados para la evaluación, la clasificación y el tratamiento de los riesgos detectados;

d) los procesos existentes para verificar que los riesgos detectados se gestionan adecuadamente;

e) los procesos utilizados para comprobar la ciberseguridad de un tipo de vehículo;

f) los procesos utilizados para garantizar que la evaluación de riesgos se mantiene actualizada;

g) los procesos utilizados para supervisar, detectar y responder a los ciberataques, las ciberamenazas y las vulnerabilidades que afectan a los tipos de vehículos, y los procesos utilizados para determinar si las medidas de ciberseguridad siguen siendo eficaces a la luz de nuevas las ciberamenazas y vulnerabilidades que se han detectado;

h) los procesos utilizados para facilitar los datos pertinentes que respalden el análisis de los intentos de ciberataques o de los ciberataques consumados.

7.2.2.3. El fabricante del vehículo demostrará que los procesos utilizados en su sistema de gestión de la ciberseguridad garantizarán que, sobre la base de la clasificación a que se refiere el punto 7.2.2.2, letras c) y g), las ciberamenazas y las vulnerabilidades que requieren por su parte se mitigan en un plazo razonable.

7.2.2.4. El fabricante del vehículo demostrará que los procesos utilizados en el marco de su sistema de gestión de la ciberseguridad garantizarán que la supervisión a que se refiere el punto 7.2.2.2, letra g), sea continua. Esta condición:

a) incluirá en la supervisión los vehículos después de la primera matriculación;

b) incluirá la capacidad para analizar y detectar ciberamenazas, vulnerabilidades y ciberataques a partir de los datos del vehículo y de los registros del vehículo. Esta capacidad respetará el punto 1.3 y los derechos de privacidad de los propietarios o los conductores del vehículo, en particular en lo referente al consentimiento.

7.2.2.5. El fabricante del vehículo deberá mostrar la forma en que su sistema de gestión de la ciberseguridad gestionará las dependencias que puedan existir con proveedores contratados, proveedores de servicios o suborganizaciones del fabricante en lo que respecta a los requisitos del punto 7.2.2.2.

7.3. Requisitos relativos a los tipos de vehículos

7.3.1. El fabricante contará con un certificado de conformidad del sistema de gestión de la ciberseguridad válido pertinente para el tipo de vehículo sujeto a homologación.

No obstante, en el caso de homologaciones de tipo anteriores al 1 de julio de 2024, si el fabricante del vehículo puede demostrar que el tipo de vehículo no se pudo desarrollar de conformidad con el sistema de gestión de la ciberseguridad, deberá demostrar entonces que la ciberseguridad se tuvo en cuenta de forma adecuada durante la fase de desarrollo del tipo de vehículo en cuestión.

7.3.2. El fabricante del vehículo determinará y gestionará los riesgos relacionados con el proveedor para el tipo de vehículo sujeto a homologación.

7.3.3. El fabricante del vehículo determinará los elementos críticos del tipo de vehículo y realizará una evaluación de riesgos exhaustiva para dicho tipo y tratará o gestionará los riesgos detectados de forma adecuada. La evaluación de riesgos tendrá en cuenta los elementos individuales del tipo de vehículo y sus interacciones. La evaluación de riesgos tendrá en cuenta también las interacciones con cualquier otro sistema externo. Al evaluar los riesgos, el fabricante del vehículo tendrá en cuenta los riesgos relacionados con todas las amenazas a que se refiere la parte A del anexo 5, así como cualquier otro riesgo pertinente.

7.3.4. El fabricante del vehículo protegerá el tipo de vehículo contra los riesgos detectados en la evaluación de riesgos que haya realizado. Se adoptarán medidas de mitigación proporcionadas para proteger el tipo de vehículo. Las medidas de mitigación aplicadas incluirán todas las medidas de este tipo a que se refieren las partes B y C del anexo 5 que sean pertinentes para los riesgos detectados. No obstante, si una medida de mitigación mencionada en la parte A o B del anexo 5 no es pertinente o suficiente para el riesgo detectado, el fabricante del vehículo se asegurará de que se aplique otra medida de mitigación adecuada.

En particular, en el caso de las homologaciones de tipo anteriores al 1 de julio de 2024, el fabricante del vehículo se asegurará de que se aplique otra medida de mitigación adecuada si una medida de mitigación mencionada en las partes B o C del anexo 5 no es técnicamente viable. El fabricante facilitará a la autoridad de homologación la correspondiente evaluación de la viabilidad técnica.

7.3.5. El fabricante del vehículo adoptará medidas adecuadas y proporcionadas para garantizar entornos específicos seguros en el tipo de vehículo (si se incluyen) para el almacenaje y la ejecución del *software*, servicios, aplicaciones o datos postventa.

7.3.6. El fabricante del vehículo llevará a cabo, antes de la homologación de tipo, ensayos adecuados y suficientes para verificar la eficacia de las medidas de seguridad aplicadas.

7.3.7. El fabricante del vehículo aplicará medidas para el tipo de vehículo a fin de:

a) detectar y prevenir ciberataques contra los vehículos del tipo de vehículo;

b) respaldar la capacidad de supervisión del fabricante del vehículo en lo que respecta a la detección de amenazas, vulnerabilidades y ciberataques relacionados con el tipo de vehículo;

c) proporcionar capacidad forense en relación con los datos a fin de permitir el análisis de los intentos de ciberataques o de los ciberataques consumados.

7.3.8. Los módulos criptográficos utilizados a los efectos del presente Reglamento estarán en consonancia con normas consensuadas. Si los módulos criptográficos utilizados no están en consonancia con normas consensuadas, el fabricante del vehículo deberá justificar su uso.

7.4. Disposiciones relativas a la notificación

7.4.1. El fabricante del vehículo notificará al menos una vez al año, o con más frecuencia si fuera pertinente, a la autoridad de homologación o al servicio técnico el resultado de sus actividades de supervisión definidas en el punto 7.2.2.2, letra g), incluida la información pertinente sobre nuevos ciberataques. El fabricante del vehículo también notificará y confirmará a la autoridad de homologación o al servicio técnico que las medidas de mitigación en materia de ciberseguridad aplicadas a sus tipos de vehículos siguen siendo eficaces, así como las medidas adicionales adoptadas.

7.4.2. La autoridad de homologación o el servicio técnico verificarán la información facilitada y, de ser necesario, exigirán al fabricante del vehículo que subsane cualquier ineficacia.

Si la notificación o la respuesta no son suficientes, la autoridad de homologación podrá decidir retirar el certificado de conformidad del sistema de gestión de la ciberseguridad de acuerdo con el punto 6.8.

8. MODIFICACIÓN DEL TIPO DE VEHÍCULO Y EXTENSIÓN DE LA HOMOLOGACIÓN DE TIPO

8.1. Toda modificación del tipo de vehículo que afecte a su rendimiento técnico en lo que respecta a la ciberseguridad o de la documentación exigida por el presente Reglamento se notificará a la autoridad de homologación que homologó el tipo de vehículo. Esta podrá entonces:

8.1.1. considerar que las modificaciones realizadas siguen cumpliendo los requisitos y la documentación de la homologación de tipo existente; o

8.1.2. proceder a la evaluación complementaria que sea necesaria en virtud del punto 5 y requerir, cuando proceda, otro informe de ensayo del servicio técnico responsable de la realización de los ensayos.

8.1.3. La confirmación, la extensión o la denegación de la homologación, especificando las alteraciones, se comunicará mediante un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento. La autoridad de homologación que expida la extensión de la homologación asignará un número de serie a dicha extensión e informará de ello a las demás Partes del Acuerdo de 1958 que apliquen el presente Reglamento por medio de un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento.

9. CONFORMIDAD DE LA PRODUCCIÓN

9.1. Los procedimientos de conformidad de la producción se ajustarán a los establecidos en el anexo 1 del Acuerdo de 1958 (E/ECE//TRANS/505/Rev.3) y cumplirán los requisitos que se exponen a continuación:

9.1.1. el titular de la homologación deberá garantizar que los resultados de los ensayos de conformidad de la producción se registran y que los documentos anejos están disponibles durante un período que se determinará de común acuerdo con la autoridad de homologación o su servicio técnico. Dicho período no será superior a diez años a partir del momento en que se produzca el cese definitivo de la producción;

9.1.2. la autoridad de homologación que haya concedido la homologación de tipo podrá verificar en cualquier momento los métodos de control de la conformidad aplicados en cada unidad de producción. La frecuencia normal de esas verificaciones será de una vez cada tres años.

10. SANCIONES POR FALTA DE CONFORMIDAD DE LA PRODUCCIÓN

10.1. La homologación concedida con respecto a un tipo de vehículo con arreglo al presente Reglamento podrá retirarse si no se cumplen los requisitos que figuran en él o si los vehículos de la muestra no cumplen los requisitos del presente Reglamento.

10.2. Cuando una autoridad de homologación retire una homologación que haya concedido previamente, informará de ello de forma inmediata a las demás Partes contratantes que apliquen el presente Reglamento mediante un formulario de comunicación conforme al modelo que figura en el anexo 2 del presente Reglamento.

11. CESE DEFINITIVO DE LA PRODUCCIÓN

11.1. Si el titular de una homologación cesa por completo de fabricar un tipo de vehículo homologado con arreglo al presente Reglamento, informará de ello a la autoridad que concedió la homologación. Tras recibir la correspondiente comunicación, dicha autoridad deberá informar de ello a las demás Partes contratantes del Acuerdo que apliquen el presente Reglamento mediante una copia del formulario de homologación al final de la cual figurará en grandes caracteres la indicación firmada y fechada «CESE DE LA PRODUCCIÓN».

12. NOMBRES Y DIRECCIONES DE LOS SERVICIOS TÉCNICOS RESPONSABLES DE REALIZAR LOS ENSAYOS DE HOMOLOGACIÓN Y DE LAS AUTORIDADES DE HOMOLOGACIÓN DE TIPO

12.1. Las Partes contratantes del Acuerdo que apliquen el presente Reglamento deberán comunicar a la Secretaría de las Naciones Unidas el nombre y la dirección de los servicios técnicos encargados de realizar los ensayos de homologación y de las autoridades de homologación de tipo que concedan la homologación y a las cuales deban remitirse los formularios expedidos en otros países que certifiquen la concesión, extensión, denegación o retirada de la homologación.

ANEXO 1

Ficha técnica

La información que figura a continuación deberá presentarse, en su caso, por triplicado e ir acompañada de un índice de contenidos. Los planos que vayan a entregarse se presentarán a la escala adecuada, suficientemente detallados y en formato A4 o doblados de forma que se ajusten a dicho formato. Si se presentan fotografías, deberán ser suficientemente detalladas.

1. Marca (nombre comercial del fabricante): .....

2. Tipo y denominación(es) comercial(es) general(es): .....

3. Medio de identificación del tipo, si está marcado en el vehículo: .....

4. Ubicación de esa marca: .....

5. Categoría(s) de vehículo: .....

6. Nombre y dirección del fabricante o del representante del fabricante: .....

7. Nombre y dirección de la(s) planta(s) de montaje: .....

8. Fotografía(s) o plano(s) de un vehículo representativo: .....

9. Ciberseguridad

9.1. Características generales de fabricación del tipo de vehículo, entre ellas:

a) los sistemas del vehículo que sean pertinentes para la ciberseguridad del tipo de vehículo;

b) los componentes de dichos sistemas que sean pertinentes para la ciberseguridad;

c) las interacciones de dichos sistemas con otros sistemas dentro del tipo de vehículo y las interfaces externas.

9.2. Una representación esquemática del tipo de vehículo.

9.3. El número del certificado de conformidad del sistema de gestión de la ciberseguridad: .....

9.4. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describe el resultado de la evaluación de riesgos y los riesgos detectados: .....

9.5. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describen las medidas de mitigación que se han aplicado en los sistemas enumerados o en el tipo de vehículo y la forma en que estas abordan los riesgos indicados: .....

9.6. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describe la protección de los entornos específicos previstos para el *software*, servicios, aplicaciones o datos postventa: .....

9.7. Documentos, relativos al tipo de vehículo cuya homologación se solicita, en los que se describen los ensayos realizados para verificar la ciberseguridad del tipo de vehículo y sus sistemas, y el resultado de dichos ensayos: .....

9.8. Descripción de la consideración de la cadena de suministro con respecto a la ciberseguridad: .....

Apéndice 1 del Anexo 1

Modelo de la declaración de conformidad del sistema de gestión de la ciberseguridad del fabricante

Declaración de conformidad del fabricante con los requisitos del sistema de gestión de la ciberseguridad

Nombre del fabricante: .....

Dirección del fabricante: .....

..... (*nombre del fabricante*) atestigua que se han instalado y se mantendrán los procesos necesarios para cumplir con los requisitos del sistema de gestión de la ciberseguridad establecidos en el punto 7.2 del Reglamento n.º 155 de las Naciones Unidas..... ....

Hecho en: ..... (*lugar*)

Fecha: .....

Nombre del firmante: .....

Cargo del firmante: .....

.....

(*Sello y firma del representante del fabricante*)

ANEXO 2

Comunicación

[Formato máximo: A4 (210 × 297 mm)]

Expedida por: Nombre de la administración:
.....
.....
.....

relativa a (2) La concesión de la homologación
La extensión de la homologación
La retirada de la homologación con efecto a partir del dd/mm/aaaa
La denegación de la homologación
Cese definitivo de la producción

de un tipo de vehículo con arreglo al Reglamento n.º 155 de las Naciones Unidas

N.º de homologación: .....

N.º de extensión: .....

Motivos de la extensión: .....

1. Marca (nombre comercial del fabricante): .....

2. Tipo y denominación(es) comercial(es) general(es) .....

3. Medio de identificación del tipo, si está marcado en el vehículo: .....

3.1. Ubicación de esa marca: .....

4. Categoría(s) de vehículo: .....

5. Nombre y dirección del fabricante o del representante del fabricante: .....

6. Nombre y dirección de la(s) planta(s) de montaje: .....

7. Número del certificado de conformidad del sistema de gestión de la ciberseguridad: .....

8. Servicio técnico encargado de realizar los ensayos: .....

9. Fecha del informe de ensayo: .....

10. Número del informe de ensayo: .....

11. Observaciones: (en su caso). .....

12. Lugar: .....

13. Fecha: .....

14. Firma: .....

15. Se adjunta el índice del expediente de homologación en posesión de la autoridad de homologación, que puede obtenerse a petición del interesado:

([1]) Táchese lo que no proceda.

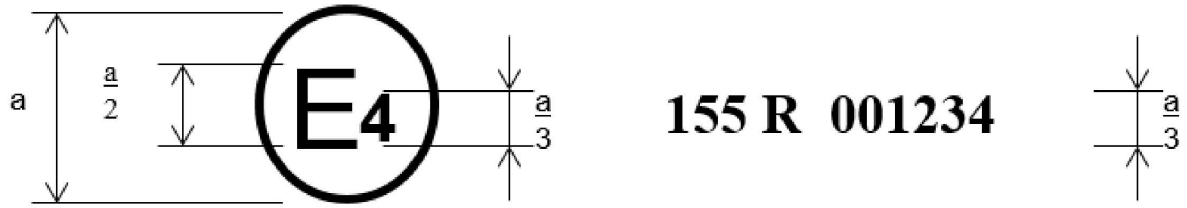
([2]) Número distintivo del país que ha concedido/extendido/denegado/retirado la homologación (véanse las disposiciones del Reglamento relativas a la homologación).:

ANEXO 3

Disposición de la marca de homologación

MODELO A

(Véase el punto 4.2 del presente Reglamento)



a = 8 mm mín.

Esta marca de homologación colocada en un vehículo indica que el tipo de vehículo de carretera en cuestión ha sido homologado en los Países Bajos (E4), con arreglo al Reglamento n.º 155 y con el número de homologación 001234. Los dos primeros dígitos del número de homologación indican que esta fue concedida de conformidad con los requisitos del presente Reglamento en su forma original (00).

ANEXO 4

Modelo de certificado de conformidad del sistema de gestión de la ciberseguridad

Certificado de conformidad del sistema de gestión de la ciberseguridad

con el Reglamento n.º 155 de las Naciones Unidas

Número del certificado [*Número de referencia*]

[……. *Autoridad de homologación*]

Certifica que

Fabricante: ……

Dirección del fabricante: ……

cumple con lo dispuesto en el punto 7.2 del Reglamento n.º 155

Los controles fueron realizados el día: ……

por (nombre y dirección de la autoridad de homologación o el servicio técnico): ……

Número del informe: ……

El certificado será válido hasta el [……*fecha*]

Hecho en [……*lugar*]

el [……*fecha*]

[……*Firma*]

Anexos: descripción del sistema de gestión de la ciberseguridad por el fabricante.

ANEXO 5

Lista de amenazas y sus correspondientes medidas de mitigación

1. Este anexo consta de tres partes. En la parte A se describe la línea de base de las amenazas, las vulnerabilidades y los métodos de ataque. En la parte B se describen las medidas de mitigación de las amenazas previstas para los tipos de vehículos. En la parte C se describen las medidas de mitigación de las amenazas previstas para aspectos ajenos al vehículo, por ejemplo, en *back-ends* de TI.

2. La parte A, la parte B y la parte C se tendrán en cuenta para las evaluaciones de riesgos y las medidas de mitigación que aplicarán los fabricantes de los vehículos.

3. En la parte A se han indexado las vulnerabilidades de alto nivel con sus correspondientes ejemplos. Se hace referencia a la misma indexación en los cuadros de las partes B y C para vincular cada ataque/vulnerabilidad con una lista de medidas de mitigación correspondientes.

4. En el análisis de las amenazas también se tendrán en cuenta los posibles efectos de los ataques. Esto puede ayudar a determinar la gravedad de un riesgo y a detectar riesgos adicionales. Los posibles efectos de un ataque pueden ser:

   a) afectación del funcionamiento seguro del vehículo;

   b) interrupción del funcionamiento de las funciones del vehículo;

   c) modificación del *software* y alteración del rendimiento;

   d) alteración del *software* pero sin efectos en el funcionamiento;

   e) violación de la integridad de los datos;

   f) violación de la confidencialidad de los datos;

   g) perdida de disponibilidad de los datos;

   h) otros, incluida la delincuencia.

Parte A. Vulnerabilidad o método de ataque relacionados con las amenazas

1. En el cuadro A1 se ofrecen descripciones generales de las amenazas y de la vulnerabilidad o el método de ataque relacionados con ellas

Cuadro A1

Lista de vulnerabilidades o métodos de ataque relacionados con las amenazas

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
4.3.1. Amenazas relativas a los servidores *back-end* en relación con vehículos sobre el terreno	1	Servidores *back-end* utilizados como medio para atacar un vehículo o extraer datos	1.1	Abuso de privilegios por parte del personal (ataque interno)
			1.2	Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por *backdoors*, vulnerabilidades de un *software* del sistema sin parches, ataques SQL u otros medios)
			1.3	Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)
	2	Interrupción de los servicios del servidor *back-end*, lo que afecta al funcionamiento de un vehículo	2.1	El ataque al servidor *back-end* interrumpe su funcionamiento, por ejemplo evita que interactúe con los vehículos y les preste servicios de los que dependen

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
	3	Los datos relacionados con el vehículo que se almacenan en los servidores *back-end* se pierden o se ven comprometidos («violación de la seguridad de los datos»)	3.1	Abuso de privilegios por parte del personal (ataque interno)
			3.2	Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando el almacenamiento de los datos corre a cargo de terceros proveedores de servicios en la nube
			3.3	Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por *backdoors*, vulnerabilidades de un *software* del sistema sin parches, ataques SQL u otros medios)
			3.4	Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)
			3.5	Violación de la seguridad de los datos por un intercambio de datos no intencionado (p. ej., errores administrativos)
4.3.2. Amenazas a vehículos por lo que respecta a sus canales de comunicación	4	Falsificación de los mensajes o datos recibidos por el vehículo	4.1	Falsificación de mensajes por suplantación de identidad (p. ej., 802.11p V2X durante la marcha en pelotón, mensajes GNSS, etc.)
			4.2	Ataque Sybil (a fin de suplantar la identidad de otros vehículos como si hubiera muchos vehículos en la carretera)
	5	Canales de comunicación utilizados para llevar a cabo una manipulación, eliminación u otras modificaciones no autorizadas del código o los datos almacenados por el vehículo	5.1	Los canales de comunicación permiten la introducción de un código, por ejemplo, se puede introducir un código binario de *software* manipulado en el flujo de comunicación
			5.2	Los canales de comunicación permiten la manipulación de los datos o el código almacenados por el vehículo
			5.3	Los canales de comunicación permiten sobreescribir los datos o el código almacenados por el vehículo
			5.4	Los canales de comunicación permiten borrar los datos o el código almacenados por el vehículo
			5.5	Los canales de comunicación permiten introducir datos o el código en el vehículo (escritura de datos/código)
	6	Los canales de comunicación permiten aceptar mensajes poco fiables o que no son de confianza o son vulnerables a secuestro de sesión o ataques de repetición	6.1	Aceptación de información de una fuente poco fiable o que no es de confianza
			6.2	Ataque de intermediario / secuestro de sesión
			6.3	Ataque de repetición, por ejemplo un ataque contra una pasarela de comunicación permite al atacante devolver a una versión anterior el *software* de una unidad de control electrónico o el *firmware* de la pasarela

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
	7	La información puede divulgarse fácilmente. Por ejemplo, mediante la interceptación de las comunicaciones o permitiendo el acceso no autorizado a archivos o carpetas confidenciales	7.1	Interceptación de la información / radiaciones interferentes / control de las comunicaciones
			7.2	Obtención de acceso no autorizado a archivos o datos
	8	Ataques de denegación de servicio a través de canales de comunicación para alterar las funciones del vehículo	8.1	Envío de una gran cantidad de datos inútiles al sistema de información del vehículo para que este no pueda prestar servicios de la forma habitual
			8.2	Ataque de agujero negro para interrumpir la comunicación entre vehículos; el atacante puede bloquear los mensajes entre los vehículos
	9	Un usuario sin privilegios puede obtener acceso privilegiado a los sistemas del vehículo	9.1	Un usuario sin privilegios puede obtener acceso privilegiado, por ejemplo acceso *root*
	10	Los virus integrados en los medios de comunicación pueden infectar los sistemas del vehículo	10.1	Un virus integrado en los medios de comunicación infecta los sistemas del vehículo
	11	Los mensajes recibidos por el vehículo (por ejemplo, mensajes X2V o mensajes de diagnóstico) o transmitidos en él contienen contenido malicioso	11.1	Mensajes internos (p. ej., CAN) maliciosos
			11.2	Mensajes V2X maliciosos, p. ej., mensajes de infraestructura a vehículo o de vehículo a vehículo (p. ej., CAM, DENM)
			11.3	Mensajes de diagnóstico maliciosos
			11.4	Mensajes propietarios maliciosos (p. ej., los que normalmente se envían desde el fabricante de equipo original o el proveedor de componentes/sistemas/funciones)
4.3.3. Amenazas a vehículos con respecto a sus procedimientos de actualización	12	Uso incorrecto o compromiso de los procedimientos de actualización	12.1	Compromiso de los procedimientos inalámbricos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*
			12.2	Compromiso de los procedimientos locales/físicos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*
			12.3	El *software* se manipula antes del proceso de actualización (y está, por tanto, corrompido), aunque el proceso de actualización esté intacto

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
			12.4	Compromiso de las claves criptográficas del proveedor de *software* para permitir una actualización inválida
	13	Es posible denegar actualizaciones legítimas	13.1	Ataque de denegación de servicio contra un servidor o red de actualización para impedir el lanzamiento de actualizaciones de *software* crítico o el desbloqueo de características específicas del cliente
4.3.4. Amenazas a vehículos con respecto a acciones humanas involuntarias que facilitan un ciberataque	15	Actores legítimos pueden actuar de forma que se facilita involuntariamente un ciberataque	15.1	Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue *software* malicioso o permita un ataque
			15.2	No se siguen los procedimientos de seguridad definidos
4.3.5. Amenazas a vehículos con respecto a su conectividad externa y sus conexiones externas	16	La manipulación de la conectividad de las funciones del vehículo permite un ciberataque que puede incluir los sistemas telemáticos; los sistemas que permiten operaciones remotas; y los sistemas que utilizan comunicaciones inalámbricas de corto alcance	16.1	Manipulación de las funciones diseñadas para operar los sistemas a distancia, como una llave de control remoto, un inmovilizador y una estación de carga
			16.2	Manipulación de los sistemas telemáticos del vehículo (p. ej., manipulación de la medición de la temperatura de mercancías delicadas, desbloqueo remoto de puertas de carga)
			16.3	Interferencia con sensores o sistemas inalámbricos de corto alcance
	17	*Software* alojado por terceros, p. ej., aplicaciones de entretenimiento utilizadas como medio para atacar los sistemas de vehículo	17.1	Aplicaciones corruptas o aplicaciones con una mala seguridad de *software* utilizadas como método para atacar los sistemas del vehículo
	18	Dispositivos conectados a interfaces externas, p. ej., puertos USB, puerto OBD, utilizados como medio para atacar los sistemas del vehículo	18.1	Interfaces externas como puertos USB u otros puertos utilizadas como punto de ataque, por ejemplo, mediante la introducción de un código
			18.2	Medios infectados con un virus conectados al vehículo
			18.3	Uso del acceso al diagnóstico (p. ej., mochilas en el puerto ODB) para facilitar un ataque, p. ej., para manipular los parámetros del vehículo (de manera directa o indirecta)
4.3.6. Amenazas a los datos o el código del vehículo	19	Extracción de los datos o el código del vehículo	19.1	Extracción de *software* propietario o protegido con derechos de autor de los sistemas del vehículo (piratería)
			19.2	Acceso no autorizado a la información personal del propietario, como su identidad, información sobre cuentas de pago, información sobre sus contactos, información sobre la ubicación, identificación electrónica del vehículo, etc.
			19.3	Extracción de claves criptográficas

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
	20	Manipulación de los datos o el código del vehículo	20.1	Cambios ilícitos o no autorizados en la identificación electrónica del vehículo
			20.2	Fraude de identidad. Por ejemplo, si un usuario desea mostrar otra identidad cuando se comunica con sistemas de peaje, un *back-end* del fabricante
			20.3	Acción para eludir los sistemas de supervisión (p. ej., piratear/manipular/ bloquear mensajes como los datos del dispositivo de seguimiento ODR-Tracker o el número de ejecuciones)
			20.4	Manipulación de datos para falsificar los datos de conducción del vehículo (p. ej., kilometraje, velocidad de conducción, instrucciones de conducción, etc.)
			20.5	Cambios no autorizados en los datos de diagnóstico del sistema
	21	Borrado de datos o de código	21.1	Borrado o manipulación no autorizados de los registros de eventos del sistema
	22	Introducción de *software* malicioso	22.2	Introducción de *software* malicioso o actividad de *software* malicioso
	23	Introducción de *software* nuevo o sobreescritura de *software* ya existente	23.1	Fabricación de *software* del sistema de control o del sistema de información del vehículo
	24	Alteración de sistemas u operaciones	24.1	Denegación del servicio, por ejemplo, esta acción puede desencadenarse en la red interna mediante la inundación de un bus CAN o la provocación de fallos en una unidad de control electrónico a través de una alta tasa de mensajes
	25	Manipulación de los parámetros del vehículo	25.1	Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave del vehículo, como los datos de freno, el umbral de despliegue de los airbags, etc.
			25.2	Acceso no autorizado para falsificar los parámetros de carga, como la tensión de carga, la potencia de carga, la temperatura de la batería, etc.
4.3.7. Posibles vulnerabilidades que podrían explotarse si no se protegen o se refuerzan de forma suficiente	26	Las tecnologías criptográficas pueden verse comprometidas o no se aplican lo suficiente	26.1	La combinación de claves de cifrado cortas y un período de validez largo permite al atacante descifrar las claves del sistema de cifrado
			26.2	Uso insuficiente de algoritmos criptográficos para proteger sistemas sensibles
			26.3	Uso de algoritmos criptográficos que ya están obsoletos o lo estarán pronto

Descripciones generales y específicas de vulnerabilidades/ amenazas			Ejemplo de vulnerabilidad o método de ataque	
	27	Las piezas o los suministros podrían verse comprometidos y permitir el ataque de los vehículos	27.1	*Hardware* o *software* diseñados para permitir un ataque o que no cumplen los criterios de diseño para detener un ataque
	28	El desarrollo de *software* o *hardware* permite vulnerabilidades	28.1	Errores de *software*. La presencia de errores de software puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el *software* no se ha probado para verificar que no contiene un mal código conocido o errores conocidos y reducir el riesgo de que contenga un mal código desconocido o errores desconocidos
			28.2	El uso de restos de la fase de desarrollo (p. ej., puertos de depuración, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de desarrolladores, etc.) puede permitir el acceso a unidades de control electrónico o permitir a los atacantes obtener mayores privilegios
	29	El diseño de la red introduce vulnerabilidades	29.1	Puertos de Internet que se dejan abiertos y dan acceso a sistemas de redes
			29.2	Eludir la separación de redes para obtener el control Un ejemplo específico es el uso de puntos de acceso o pasarelas no protegidas (como pasarelas camión-remolque) para eludir las protecciones y obtener acceso a otros segmentos de la red con vistas a llevar a cabo actos malintencionados, como enviar mensajes de bus CAN arbitrarios
	31	Puede producirse una transmisión de datos no deseada	31.1	Violación de la seguridad de los datos. Pueden filtrarse datos personales cuando el coche cambia de usuario (p. ej., cuando se vende o se usa como vehículo de alquiler con nuevos arrendatarios)
	32	La manipulación física de los sistemas puede posibilitar un ataque	32.1	Manipulación del *hardware* electrónico, p. ej., la instalación de *hardware* electrónico no autorizado en un vehículo para posibilitar un ataque de intermediario Sustitución de *hardware* electrónico autorizado (p. ej., sensores) por *hardware* electrónico no autorizado Manipulación de la información recogida por un sensor (por ejemplo, utilizando un imán para manipular el sensor de efecto Hall conectado a la caja de cambios)

Parte B. Medidas de mitigación de las amenazas dirigidas a vehículos

1. Medidas de mitigación para los «canales de comunicación del vehículo»

Las medidas de mitigación de las amenazas relacionadas con los «canales de comunicación del vehículo» se enumeran en el cuadro B1

Cuadro B1

Medidas de mitigación de las amenazas relacionadas con los «canales de comunicación del vehículo»

Referencia al cuadro A1	Amenazas para los «canales de comunicación del vehículo»	Ref.	Medida de mitigación
4.1	Falsificación de mensajes (p. ej., 802.11p V2X durante la marcha en pelotón, mensajes GNSS, etc.) mediante la suplantación de identidad	M10	El vehículo verificará la autenticidad e integridad de los mensajes que recibe
4.2	Ataque Sybil (a fin de suplantar la identidad de otros vehículos como si hubiera muchos vehículos en la carretera)	M11	Se implantarán controles de seguridad para almacenar claves criptográficas (p. ej., uso de módulos de seguridad de *hardware*)
5.1	Los canales de comunicación permiten la introducción de un código en los datos o el código del vehículo, por ejemplo, se puede introducir un código binario de *software* en el flujo de comunicación	M10 M6	El vehículo verificará la autenticidad e integridad de los mensajes que recibe Los sistemas incorporarán seguridad desde el diseño para minimizar riesgos
5.2	Los canales de comunicación permiten la manipulación de los datos o el código almacenados por el vehículo	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos y el código del sistema
5.3	Los canales de comunicación permiten sobreescribir los datos o el código almacenados por el vehículo		
5.4 21.1	Los canales de comunicación permiten borrar los datos o el código almacenados por el vehículo		
5.5	Los canales de comunicación permiten introducir datos o un código en los sistemas del vehículo (escribir código de datos)		
6.1	Aceptación de información de una fuente poco fiable o que no es de confianza	M10	El vehículo verificará la autenticidad e integridad de los mensajes que recibe
6.2	Ataque de intermediario / secuestro de sesión	M10	El vehículo verificará la autenticidad e integridad de los mensajes que recibe
6.3	Ataque de repetición, por ejemplo, un ataque contra una pasarela de comunicación permite al atacante devolver a una versión anterior el *software* de una unidad de control electrónico o el *firmware* de la pasarela		
7.1	Interceptación de la información / radiaciones interferentes / control de las comunicaciones	M12	Se protegerán los datos confidenciales transmitidos al vehículo o desde este
7.2	Obtención de acceso no autorizado a archivos o datos	M8	Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema. El Proyecto de seguridad de aplicaciones web abiertas (OWASP) ofrece ejemplos de controles de seguridad

Referencia al cuadro A1	Amenazas para los «canales de comunicación del vehículo»	Ref.	Medida de mitigación
8.1	Envío de un gran número de datos inútiles al sistema de información del vehículo para que este no pueda prestar servicios de la forma habitual	M13	Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio
8.2	Ataque de agujero negro, interrupción de la comunicación entre vehículos mediante el bloqueo de la transmisión de mensajes a otros vehículos	M13	Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio
9.1	Un usuario sin privilegios puede obtener acceso privilegiado, por ejemplo, acceso *root*	M9	Se emplearán medidas para prevenir y detectar accesos no autorizados
10.1	Un virus integrado en los medios de comunicación infecta los sistemas del vehículo	M14	Deben considerarse medidas para proteger los sistemas frente a virus o *software* malicioso integrados
11.1	Mensajes internos maliciosos (p. ej., CAN)	M15	Deben considerarse medidas para detectar actividad o mensajes internos maliciosos
11.2	Mensajes V2X maliciosos, p. ej., mensajes de infraestructura a vehículo o de vehículo a vehículo (CAM, DENM)	M10	El vehículo verificará la autenticidad e integridad de los mensajes que recibe
11.3	Mensajes de diagnóstico maliciosos		
11.4	Mensajes propietarios maliciosos (p. ej., los que normalmente se envían desde el fabricante de equipo original o el proveedor de componentes/sistemas/funciones)		

2. Medidas de mitigación para el «proceso de actualización»

Las medidas de mitigación de las amenazas relacionadas con el «proceso de actualización» se enumeran en el cuadro B2

Cuadro B2

Medidas de mitigación de las amenazas relacionadas con el «proceso de actualización»

Referencia al cuadro A1	Amenazas para el «proceso de actualización»	Ref.	Medida de mitigación
12.1	Compromiso de los procedimientos inalámbricos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*	M16	Se emplearán procedimientos seguros de actualización del *software*
12.2	Compromiso de los procedimientos locales/físicos de actualización de *software*. Esto incluye la falsificación del programa de actualización del sistema o *firmware*		
12.3	El *software* se manipula antes del proceso de actualización (y está, por tanto, corrompido), aunque el proceso de actualización esté intacto		

Referencia al cuadro A1	Amenazas para el «proceso de actualización»	Ref.	Medida de mitigación
12.4	Compromiso de las claves criptográficas del proveedor de *software* para permitir una actualización inválida	M11	Se aplicarán controles de seguridad para almacenamiento de claves criptográficas
13.1	Ataque de denegación de servicio contra un servidor o red de actualización para impedir el lanzamiento de actualizaciones de *software* crítico o el desbloqueo de características específicas del cliente	M3	Se aplicarán controles de seguridad a los sistemas de *back-end*. Cuando los servidores *back-end* son esenciales para la prestación de los servicios, existen medidas de recuperación en caso de interrupción del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad

3. Medidas de mitigación para las «acciones humanas involuntarias que facilitan un ciberataque»

Las medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias que facilitan un ciberataque» se enumeran en el cuadro B3.

Cuadro B3

Medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias que facilitan un ciberataque»

Referencia al cuadro A1	Amenazas relacionadas con «acciones humanas involuntarias»	Ref.	Medida de mitigación
15.1	Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue *software* malicioso o permita un ataque	M18	Se aplicarán medidas para definir y controlar las funciones de usuario y los privilegios de acceso, sobre la base del principio del mínimo privilegio de acceso
15.2	No se siguen los procedimientos de seguridad definidos	M19	Las organizaciones garantizarán la definición y el cumplimiento de los procedimientos de seguridad, incluido el registro de actividades y el acceso relacionados con la gestión de las funciones de seguridad

4. Medidas de mitigación para «la conectividad externa y las conexiones externas»

Las medidas de mitigación de las amenazas relacionadas con «la conectividad externa y las conexiones externas» se enumeran en el cuadro B4

Cuadro B4

Medidas de mitigación de las amenazas relacionadas con «la conectividad externa y las conexiones externas»

Referencia al cuadro A1	Amenazas para «la conectividad externa y las conexiones externas»	Ref.	Medida de mitigación
16.1	Manipulación de las funciones diseñadas para operar los sistemas a distancia, como una llave de control remoto, un inmovilizador y una estación de carga	M20	Se aplicarán controles de seguridad a los sistemas que tienen acceso remoto
16.2	Manipulación de los sistemas telemáticos del vehículo (p. ej., manipulación de la medición de la temperatura de mercancías delicadas, desbloqueo remoto de puertas de carga)		

Referencia al cuadro A1	Amenazas para «la conectividad externa y las conexiones externas»	Ref.	Medida de mitigación
16.3	Interferencia con sensores o sistemas inalámbricos de corto alcance		
17.1	Aplicaciones corruptas, o aplicaciones con una mala seguridad de *software* utilizadas como método para atacar los sistemas del vehículo	M21	Se evaluará la seguridad del software, se autentificará y se protegerá su integridad. Se aplicarán controles de seguridad para minimizar el riesgo procedente del *software* de terceros que está destinado a ser alojado en el vehículo o es susceptible de ser alojado en el vehículo
18.1	Interfaces externas como puertos USB u otros puertos utilizadas como punto de ataque, por ejemplo, mediante la introducción de un código	M22	Se aplicarán controles de seguridad a las interfaces externas
18.2	Medios infectados con virus conectados al vehículo		
18.3	Uso del acceso al diagnóstico (p. ej., mochilas en el puerto ODB) para facilitar un ataque, p. ej., para manipular los parámetros del vehículo (de manera directa o indirecta)	M22	Se aplicarán controles de seguridad a las interfaces externas

5. Medidas de mitigación para los «objetivos potenciales de un ataque o motivaciones para un ataque»

Las medidas de mitigación de las amenazas relacionadas con los «objetivos potenciales de un ataque o motivaciones para un ataque» se enumeran en el cuadro B5.

Cuadro B5

Medidas de mitigación de las amenazas relacionadas con los «objetivos potenciales de un ataque o motivaciones para un ataque»

Referencia al cuadro A1	Amenazas relacionadas con «objetivos potenciales de un ataque o motivaciones para un ataque»	Ref.	Medida de mitigación
19.1	Extracción de *software* patentado o protegido con derechos de autor de los sistemas del vehículo (piratería)	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad
19.2	Acceso no autorizado a la información personal del propietario, como su identidad, información sobre cuentas de pago, información sobre sus contactos, información sobre la ubicación, identificación electrónica del vehículo, etc.	M8	Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad
19.3	Extracción de claves criptográficas	M11	Se implantarán controles de seguridad para el almacenaje de claves criptográficas, p. ej., uso de módulos de seguridad
20.1	Cambios ilícitos o no autorizados en la identificación electrónica del vehículo	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad
20.2	Fraude de identidad. Por ejemplo, si un usuario desea mostrar otra identidad cuando se comunica con sistemas de peaje o *back-end* del fabricante		
20.3	Acción para eludir los sistemas de supervisión (p. ej., piratear/manipular/bloquear mensajes como los datos del dispositivo de seguimiento ODR-Tracker o el número de ejecuciones)	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad.

Referencia al cuadro A1	Amenazas relacionadas con «objetivos potenciales de un ataque o motivaciones para un ataque»	Ref.	Medida de mitigación
20.4	Manipulación de datos para falsificar los datos de conducción del vehículo (p. ej., kilometraje, velocidad de conducción, instrucciones de conducción, etc.)		Los ataques de manipulación de datos en sensores o datos transmitidos podrían mitigarse correlacionando los datos de diferentes fuentes de información
20.5	Cambios no autorizados en los datos de diagnóstico del sistema		
21.1	Borrado o manipulación no autorizados de los registros de eventos del sistema	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad.
22.2	Introducción de *software* malicioso o actividad de *software* malicioso	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad.
23.1	Fabricación de *software* del sistema de control o del sistema de información del vehículo		
24.1	Denegación del servicio, por ejemplo, esta acción puede desencadenarse en la red interna mediante la inundación de un bus CAN o la provocación de fallos en una unidad de control electrónico a través de una alta tasa de mensajes	M13	Se emplearán medidas para la detección y recuperación de un ataque de denegación de servicio
25.1	Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave del vehículo, como los datos de freno, el umbral de despliegue de los airbags, etc.	M7	Se aplicarán diseños y técnicas de control de acceso para proteger los datos o el código del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad
25.2	Acceso no autorizado para falsificar los parámetros de carga, como la tensión de carga, la potencia de carga, la temperatura de la batería, etc.		

6. Medidas de mitigación para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»

Las medidas de mitigación de las amenazas relacionadas con las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente» se enumeran en el cuadro B6.

Cuadro B6

Medidas de mitigación de las amenazas relacionadas con las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»

Referencia al cuadro A1	Amenazas para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»	Ref.	Medida de mitigación
26.1	La combinación de claves de cifrado cortas y un período de validez largo permite al atacante descifrar las claves del sistema de cifrado	M23	Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de *software* y *hardware*

Referencia al cuadro A1	Amenazas para las «posibles vulnerabilidades que podrían ser aprovechadas si no se protegen o se refuerzan de forma suficiente»	Ref.	Medida de mitigación
26.2	Uso insuficiente de algoritmos criptográficos para proteger sistemas sensibles		
26.3	Uso de algoritmos criptográficos obsoletos		
27.1	*Hardware* o *software* diseñados para permitir un ataque o que no cumplen los criterios de diseño para detener un ataque	M23	Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de *software* y *hardware*
28.1	La presencia de errores de *software* puede ser la base de posibles vulnerabilidades aprovechables. Esto se aplica sobre todo si el *software* no se ha probado para verificar que no contiene un mal código conocido o errores conocidos y reducir el riesgo de que contenga un mal código desconocido o errores desconocidos	M23	Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de *software* y *hardware*. Ensayos de ciberseguridad con una cobertura adecuada
28.2	El uso de restos de la fase de desarrollo (p. ej., puertos de depuración, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de desarrolladores, etc.) puede permitir a un atacante acceder a las unidades de control electrónico u obtener mayores privilegios		
29.1	Puertos de Internet que se dejan abiertos y dan acceso a sistemas de redes		
29.2	Eludir la separación de redes para obtener el control. Un ejemplo específico es el uso de puntos de acceso o pasarelas no protegidas (como pasarelas camión-remolque) para eludir las protecciones y obtener acceso a otros segmentos de la red con vistas a llevar a cabo actos malintencionados, como enviar mensajes de bus CAN arbitrarios	M23	Se seguirán las mejores prácticas de ciberseguridad en el desarrollo de *software* y *hardware*. Se seguirán las mejores prácticas de ciberseguridad para el diseño de sistemas y la integración de sistemas

7. Medidas de mitigación para la «pérdida de datos/violación de la seguridad de los datos del vehículo»

Las medidas de mitigación de las amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo» se enumeran en el cuadro B7.

Cuadro B7

Medidas de mitigación de las amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo»

Referencia al cuadro A1	Amenazas relacionadas con la «pérdida de datos / violación de la seguridad de los datos del vehículo»	Ref.	Medida de mitigación
31.1	Violación de la seguridad de los datos. Se puede violar la seguridad de los datos personales cuando el coche cambia de usuario (p. ej., cuando se vende o se usa como vehículo de alquiler con nuevos arrendatarios)	M24	Para el almacenamiento de datos personales se seguirán las mejores prácticas para la protección de la integridad y la confidencialidad de los datos.

8. Medidas de mitigación para la «manipulación física de los sistemas para permitir un ataque»

Las medidas de mitigación de las amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque» se enumeran en el cuadro B8.

Cuadro B8

Medidas de mitigación de las amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque»

Referencia al cuadro A1	Amenazas relacionadas con la «manipulación física de los sistemas para permitir un ataque»	Ref.	Medida de mitigación
32.1	La manipulación del *hardware* del fabricante de equipo original, p. ej., la instalación de *hardware* no autorizado en un vehículo para posibilitar un ataque de intermediario	M9	Se emplearán medidas para prevenir y detectar accesos no autorizados

Parte C. Medidas de mitigación de las amenazas externas al vehículo

1. Medidas de mitigación para los «servidores *back-end*»

Las medidas de mitigación de las amenazas relacionadas con los «servidores *back-end*» se enumeran el cuadro C1

Cuadro C1

Medidas de mitigación de las amenazas relacionadas con los «servidores *back-end*»

Referencia al cuadro A1	Amenazas para «servidores back-end»	Ref.	Medida de mitigación
1.1 y 3.1	Abuso de privilegios por parte del personal (ataque interno)	M1	Se aplican controles de seguridad a los sistemas de *back-end* para minimizar el riesgo de un ataque interno
1.2 y 3.3	Acceso no autorizado al servidor a través de Internet (posibilitado, por ejemplo, por *backdoors*, vulnerabilidades de un *software* del sistema sin parches, ataques SQL u otros medios)	M2	Se aplican controles de seguridad a los sistemas de *back-end* para minimizar accesos no autorizados. El proyecto OWASP ofrece ejemplos de controles de seguridad
1.3 y 3.4	Acceso físico no autorizado al servidor (por ejemplo, mediante memorias USB u otros medios de conexión al servidor)	M8	Mediante el diseño del sistema y el control de acceso, no debe ser posible que el personal no autorizado acceda a datos personales o a los datos críticos del sistema
2.1	El ataque al servidor *back-end* interrumpe su funcionamiento, por ejemplo evita que interactúe con los vehículos y les preste servicios de los que dependen	M3	Se aplican controles de seguridad a los sistemas de *back-end*. Cuando los servidores *back-end* son esenciales para la prestación de los servicios, existen medidas de recuperación en caso de interrupción del sistema. El proyecto OWASP ofrece ejemplos de controles de seguridad
3.2	Pérdida de información en la nube. Pueden perderse datos sensibles debido a ataques o accidentes cuando el almacenamiento de los datos corre a cargo de terceros proveedores de servicios en la nube	M4	Se aplican controles de seguridad para minimizar los riesgos asociados a la computación en la nube. En el proyecto OWASP y en las orientaciones sobre computación en la nube del Centro de Ciberseguridad Nacional (NCSC) pueden encontrarse ejemplos de controles de seguridad
3.5	Violación de la seguridad de los datos por un intercambio de datos no intencionado (p. ej., errores administrativos y almacenamiento de datos en servidores situados en garajes)	M5	Se aplican controles de seguridad a los sistemas de *back-end* para evitar violaciones de la seguridad de los datos. El proyecto OWASP ofrece ejemplos de controles de seguridad

2. Medidas de mitigación para las «acciones humanas involuntarias»

Las medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias» se enumeran en el cuadro C2.

Cuadro C2

Medidas de mitigación de las amenazas relacionadas con las «acciones humanas involuntarias»

Referencia al cuadro A1	Amenazas relacionadas con «acciones humanas involuntarias»	Ref.	Medida de mitigación
15.1	Se engaña a una víctima inocente (p. ej., un propietario, un operario o un ingeniero de mantenimiento) para que inicie una acción de tal manera que, de forma no intencionada, cargue *software* malicioso o permita un ataque	M18	Se aplicarán medidas para definir y controlar las funciones de usuario y los privilegios de acceso, sobre la base del principio del mínimo privilegio de acceso
15.2	No se siguen los procedimientos de seguridad definidos	M19	Las organizaciones garantizarán la definición y el cumplimiento de los procedimientos de seguridad, incluido el registro de actividades y el acceso relacionados con la gestión de las funciones de seguridad

3. Medidas de mitigación para la «pérdida física de datos»

Las medidas de mitigación de las amenazas relacionadas con la «pérdida física de datos» se enumeran en el cuadro C3.

Cuadro C3

Medidas de mitigación de las amenazas relacionadas con la «pérdida física de datos»

Referencia al cuadro A1	Amenazas para la «pérdida física de datos»	Ref.	Medida de mitigación
30.1	Daños causados por un tercero. Pueden perderse datos sensibles o verse comprometidos debido a daños físicos en caso de accidentes de tráfico o robos	M24	Para el almacenamiento de datos personales se seguirán las mejores prácticas para la protección de la integridad y la confidencialidad de los datos. En la norma ISO/SC27/WG5 se ofrecen ejemplos de controles de seguridad
30.2	Pérdida derivada de conflictos en la gestión de derechos digitales. Pueden borrarse datos de usuario por cuestiones relativas a la gestión de derechos digitales		
30.3	La integridad de los datos sensibles se puede perder debido al desgaste de componentes informáticos, lo que puede provocar problemas en cascada (en caso de alteración de claves, por ejemplo)		