TLP:CLEAR

Nuevas normativas de 2024 de ciberseguridad para vehículos

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junio 2024

INCIBE-CERT_GUIA_NORMATIVAS_CIBERSEGURIDAD_2024_VEHICULOS_v1.0

Índice

ÍNDICE DE FIGURAS

1. Sobre esta guía

El objetivo de esta guía es proporcionar información que ayude a entender la nueva regulación emitida por el Foro mundial para la armonización de la reglamentación sobre vehículos (WP.29), un cuerpo de la Comisión Económica de las Naciones Unidas para Europa (UNECE), referida a la ciberseguridad en vehículos, así como la presentación de consejos que ayuden a su cumplimiento.

Esta regulación consiste en dos reglamentos, el R155 y R156, que estipulan los requisitos de ciberseguridad que los fabricantes **deberán cumplir para optar a la homologación** de vehículos que vayan a circular en los países de la Unión Europea, o países fuera de la UE que adopten dichos reglamentos. En concreto, **la R155, concierne a los requisitos para la gestión de la ciberseguridad**, mientras que la **R156, estipula los requisitos para la gestión de actualizaciones de *software***.

Durante la guía, se introducen los requisitos descritos en ambos reglamentos, junto a las recomendaciones e indicaciones sobre cómo cumplirlos correctamente y qué procedimientos internos de fabricantes y proveedores pueden verse afectados por las nuevas normativas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

2. Introducción

El sector automovilístico es un ejemplo internacional de integración de tecnologías clásicas y sistemas interconectados modernos. Para hacer frente a un mercado altamente competitivo, los fabricantes han ido incorporando progresivamente más tecnología inteligente en los nuevos modelos de automóviles, desde cierres centralizados, hasta *software* de aparcamiento y conducción autónoma. Todos estos elementos pueden facilitar el uso y seguridad de un automóvil, pero, como pasa en todos los entornos industriales, cuando se introducen nuevas tecnologías, también introducen nuevos vectores de riesgo de ciberseguridad.

Por ejemplo, un automóvil con *software* vulnerable puede ser objetivo de ataques que irían desde la filtración de datos sensibles de los usuarios (datos de ubicación, hábitos de uso…), hasta poner un peligro la seguridad del conductor, los pasajeros o el resto de los ocupantes de la vía. Los riesgos se incrementan según aumenta la dependencia del automóvil de sistemas digitales para la gestión de combustible, frenos, dirección y otros elementos que lo componen.

Este nuevo paradigma ha instado una iniciativa de la Unión Europea para establecer **regulaciones estandarizadas** para todos los automóviles vendidos en el espacio europeo, sin importar fabricante o tipología de vehículo. Este esfuerzo se ha materializado en los reglamentos europeos **UN R155** y **UN R156**, reglas que entrarán en vigor **en julio de 2024**. Estas regulaciones establecen un sistema de homologación de ciberseguridad que todos los vehículos **deberán superar antes de poder ser vendidos** en la dentro de la Unión Europea. Con objetivo de ayudar a fabricantes y usuarios, en esta guía se resume el origen y objetivo de estas normas, sus elementos clave y sus implicaciones para el sector automovilístico.

Cómo afrontar los nuevos riesgos de seguridad de los vehículos ‘inteligentes’ ha sido, y sigue siendo, un debate en la industria automovilística global. Para evitar que el mercado europeo se viese ocupado por múltiples tecnologías en conflicto o que pudieran poner en peligro a los usuarios y viandantes, la UNECE (Comisión Económica de las Naciones Unidas para Europa) estableció el **Foro mundial para la armonización de la reglamentación sobre vehículos** (más conocido por su código de grupo de trabajo en la comisión: **WP.29**).

En este foro de la UNECE se reúnen, no solo representantes de los países miembros de la Unión Europea, si no también delegados de fabricantes y países críticos para la industria automovilística europea y global. El WP.29 establece debates y comités de trabajo que lideran la elaboración de regulaciones y estándares automovilísticos con el objetivo de asegurar la coordinación entre países y fabricantes, de forma que un automóvil pueda venderse y utilizarse en cualquier país asociado al estándar, con el mismo nivel de seguridad.

Aunque el WP.29 trata múltiples temas: seguridad pasiva de los elementos del diseño del vehículo, emisión de ruido y contaminantes, características de los neumáticos… Muchos de sus esfuerzos en los últimos años se han enfocado en el reto de la ciberseguridad en

vehículos, con el objetivo de adelantarse a los potenciales riesgos que supondría una adopción desorganizada e improvisada de las nuevas tecnologías en los nuevos vehículos.

Para ello, se han adoptado conceptos probados de la ciberseguridad en entornos industriales, una visión integral de la ciberseguridad que engloba todos los aspectos del fabricante y del producto final en un sistema de gestión. Esto quiere decir que todos los elementos del sistema electrónico del vehículo deben tener en cuenta cómo afectan a la ciberseguridad del conjunto, de la misma forma que todos los elementos de la cadena de suministro deben participar para asegurar el nivel de ciberseguridad objetivo en el resto de las fases del ciclo de vida del vehículo.

También, se considera que la ciberseguridad se crea en la operativa diaria, por lo que las medidas de seguridad son de poca utilidad si no se configuran y se gestionan durante todo el ciclo de vida del sistema. Para ello, la normativa también establece requisitos para la gestión de la ciberseguridad en los sistemas del vehículo y en su relación con el fabricante y el usuario final durante su mantenimiento tras la compra inicial.

Este enfoque se materializa en la homologación de ciberseguridad para vehículos. A la homologación ya establecida para los riesgos regidos por la legislación actual, señalizada por el símbolo de una ‘E’:

Figura 1: Símbolo de vehículo homologado

Un vehículo con esta homologación debe contar también con los indicadores de los riesgos (regulaciones) para los que está homologado. De esta forma, tras la entrada en vigor de la nueva regulación, los vehículos deberán contar con los códigos R155 (gestión de la ciberseguridad) y R156 (gestión de las actualizaciones de ciberseguridad).

3. Organización del documento

El presente documento se divide en dos partes principales, una dedicada a cada una de las nuevas regulaciones.

En el apartado '***4.R155: Gestión de la ciberseguridad*** 'se describen los puntos principales de la regulación **R155,** enfocada en los requisitos de ciberseguridad para el **sistema de gestión de la ciberseguridad** del vehículo. Se explica brevemente el proceso para homologar un nuevo tipo de vehículo antes de hacer un recorrido por todos los requisitos de la regulación, junto a recomendaciones y observaciones para cada uno.

Igual que en la regulación, los requisitos se han separado en:

- Requisitos para el sistema de gestión. Es decir, requisitos más enfocados a nivel del fabricante y los procesos internos (diseño, aprovisionamiento, fabricación y mantenimiento).
- Requisitos para cada tipo de vehículo, a cumplir por tipo de vehículo que se quiera homologar.

Cabe destacar el apartado '***4.2.2 Medidas de mitigación'*** donde se han recogido las medidas de mitigación generales recomendadas por la regulación, acompañadas de recomendaciones y ejemplos breves de aplicación.

El apartado '***5 R156: Actualización de software'*** realiza el mismo recorrido, esta vez enfocándose en la regulación **R156**, orientada a los requisitos de ciberseguridad para el **mantenimiento y actualización del *software* del vehículo**. Dado que muchos aspectos son redundantes entre las dos regulaciones, este apartado se ha enfocado principalmente en aquellos requisitos y controles únicos para la R156.

El documento concluye con una breve reflexión sobre la importancia de la gestión integral de la ciberseguridad durante la vida útil del vehículo, desde diseño, hasta retirada, para el correcto cumplimiento de la norma.

4. R155: Gestión de la ciberseguridad

El objetivo principal de la regulación R155 es definir los requisitos a cumplir por el vehículo y el fabricante para considerar que presenta un nivel de ciberseguridad adecuado frente a las amenazas de ciberseguridad recogidas en el anexo 5 de la homologación.

Para optar a la homologación de un tipo de vehículo concreto, el fabricante deberá, como evidencia principal de cumplimiento de los requisitos, presentar la información solicitada en el Anexo 1 de la norma (Figura 2). Como se puede observar, existe información descriptiva que el fabricante debería poder proporcionar, como los esquemas de conexión o el listado de sistemas desplegados en el vehículo, entre otros.

Sin embargo, también se requiere información relativa a los requisitos de ciberseguridad de la regulación: gestión del riesgo, medidas de mitigación del riesgo y ciberseguridad en la cadena de suministro. Estos requisitos se centran en el **sistema de gestión de la ciberseguridad del vehículo (SGSI)**, es decir, cómo se organiza y ejecuta la ciberseguridad, no sólo a nivel del vehículo y sus sistemas, también incluye en su alcance la ciberseguridad en los servidores del fabricante, su proceso de diseño y fabricación, sus capacidades para mantenimiento, monitorización y vigilancia, la gestión de vulnerabilidades y la gestión de la cadena de suministros.

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: .....

Figura 2: Anexo 1 de la regulación R155. Información a aportar por el fabricante

4.1. Cómo homologar un tipo de vehículo

Para optar a la homologación, el fabricante deberá someterse primero a un control de documentos. Para ello, el fabricante deberá presentar documentación que evidencie:

- *La correcta **gestión de riesgos a lo largo de la cadena de suministros** del vehículo.*
- *Que se ha realizado un **análisis de riesgos durante el desarrollo del vehículo** y se han mitigado los riesgos encontrados.*
- *Que las **medidas de seguridad** descritas durante la etapa de diseño a raíz del análisis de riesgo se han aplicado y probado en el vehículo.*
- *Que existe un **procedimiento para detectar y responder a amenazas** de ciberseguridad relacionadas con el vehículo.*
- *Que se registran los **datos pertinentes para contar con capacidades de detección de ciberataques y de análisis forense** posterior a un ciberataque*.

Además, una vez superado el control de documentos, el organismo homologador (o el servicio técnico sobre el que se delegue la responsabilidad) realizará una batería de pruebas técnicas en un muestreo de vehículos del tipo que se quiera homologar.

A nivel de detalle, la regulación destaca las normas ISO/SAE 21434, ISO 26262-2018 e ISO/PAS21448, como certificaciones reconocidas para los responsables de auditorías de vehículos de cara a la homologación. Aunque esta estipulación no se aplica directamente a los fabricantes, el conocimiento de estas normas puede informar en los procesos de evaluación interna previos a la homologación.

4.2. Requisitos del sistema de gestión de la ciberseguridad

Para superar este requisito, será necesario demostrar que:

El fabricante del vehículo cuenta con un sistema de gestión de la ciberseguridad (SGSI).

El SGSI es el conjunto de políticas, procedimientos y medidas que el fabricante implementa, no solo en el vehículo, si no en su propia organización, para cumplir las necesidades de ciberseguridad. Normalmente, está gobernado por una política central de ciberseguridad que describe los procesos generales en la organización, acompañada por procedimientos específicos para los diferentes aspectos de la ciberseguridad (respuesta ante incidentes, protección de datos, gestión de equipos, etc.). Cada procedimiento describe los roles y responsabilidades a desarrollar y las medidas técnicas utilizadas en el proceso.

Para que **el SGSI sea efectivo, debe ser conocido e involucrar a toda la entidad**. Requiere que la dirección esté comprometida, para asignar los recursos necesarios para su implantación, así como que el personal que asume responsabilidades de ciberseguridad tenga las capacidades y recursos para llevarlas a cabo. Además, requiere que el resto de los empleados y el personal externo conozca los procedimientos y buenas prácticas para ayudar a mantener el nivel de ciberseguridad objetivo.

Para el desarrollo del SGSI, además de estudiar los requisitos de la regulación R155, se recomienda a los fabricantes seguir las buenas prácticas definidas por la ISO 27001 o la IEC 62443 2-1.

4.2.1. Alcance del SGSI

Según la R155, el SGSI deberá aplicarse a las siguientes fases del ciclo de vida del vehículo:

1) **La fase de desarrollo**.

La regulación R155 estipula la necesidad de realizar un análisis de riesgos en la fase de diseño, para que los fabricantes puedan definir desde un inicio los requisitos de seguridad a incluir en el diseño.
Además, tener en cuenta la ciberseguridad desde el diseño del vehículo, permite al fabricante definir cómo se cumplirán otras necesidades de ciberseguridad:

- *emplear metodologías de desarrollo **seguro de software**,*
- *seleccionar **métodos de comunicación segura** entre los elementos del vehículo y con elementos externos,*
- *definir **entornos seguros para la ejecución del software** del vehículo,*
- *definir **requisitos de ciberseguridad** para la cadena de suministro.*

2) **La fase de producción.**

Durante esta fase, los procesos de ciberseguridad se enfocan en la operativa de la planta de producción y la cadena de suministro, donde el fabricante deberá:

- *aplicar los **procedimientos internos** para la ciberseguridad en el día a día de la producción,*
- *asegurar que los **proveedores y terceros** involucrados conocen y cumplen los requisitos de ciberseguridad asignados.*
- *realizar **pruebas técnicas** de las medidas de seguridad del vehículo.*

3) **La fase de posproducción.**

Las responsabilidades de ciberseguridad del fabricante no terminan tras la venta del vehículo. La incorporación de *software* en el vehículo implica la necesidad de:

- ***detectar y gestionar vulnerabilidades**, desarrollar actualizaciones de seguridad y suministrarlas a los clientes,*
- *realizar una **vigilancia activa de las amenazas** y riesgos de ciberseguridad y proporcionar una respuesta temprana a posibles incidentes y ciberataques.*

4.2.2. Medidas de mitigación

En la siguiente tabla se recopilan las medidas de mitigación descritas en la regulación y que deberán ser incluidas en el SGSI. Dado que estas medidas son bastante generales y abiertas a interpretación, se ha añadido una columna de recomendaciones o ejemplos generales para facilitar su comprensión e implantación.

Ref.	Medidas de mitigación	Recomendaciones y ejemplos generales
M1	Controles de seguridad en los sistemas ***backend**:* **ataques internos**	• Restringir el uso de usuarios con privilegios elevados, usuarios genéricos y usuarios compartidos. • Mantener una correcta gestión de cuentas de usuario. • Mantener y monitorizar registros de actividad de usuarios.

M2	Controles de seguridad para los servidores ***backend***: **control de accesos**	• Solicitar autenticación para acceder a servidores *backend*. • Aplicar política de contraseñas seguras. • Solicitar múltiples factores de autenticación. • Recoger y monitorizar registros de accesos.
M3	Controles de seguridad para los servidores ***backend***: medidas de **recuperación en caso de interrupció**n de sistemas	• Establecer guías de restauración segura de sistemas. • Mantener copias de seguridad actualizadas. • Mantener las soluciones de software actualizadas y en vigencia. • Establecer medidas de redundancia.
M4	Controles de seguridad para minimizar los riesgos de la **computación en la nube**	• Utilizar comunicaciones cifradas y cifrado de información almacenada. • Asegurar el aislamiento de los servidores en la nube de los utilizados para otras funciones o entidades. • Monitorizar los servidores remotos, gestionar y analizar las alertas de seguridad. • No dejar accesos públicos abiertos innecesarios.
M5	Controles de seguridad para los servidores ***backend***: evitar violaciones de la **seguridad de los datos**	• Control de accesos físicos a servidores. • Política de clasificación y tratamiento de información sensible. • Monitorizar de la información almacenada.
M6	**Seguridad por diseño**	• Restringir canales de comunicación innecesarios o no protegidos. • Segmentación de redes. • Seguridad en profundidad, por capas.
M7	**Control de acceso**	• Control de autenticación de usuarios. • Aplicar política de contraseñas seguras. • Recopilación de registros de accesos.
M8	**Control de acceso a datos** personales o críticos	• Autenticación de usuarios. • Uso de múltiples factores de autenticación para usuarios. • Registros de actividad de usuarios.
M9	**Prevenir y detectar accesos no autorizados**	• Monitorización de registros de accesos. • Bloqueo de cuentas ante múltiples intentos de acceso fallidos.
M10	Verificación de **autenticidad e integridad de mensajes** entrantes al vehículo	• Uso de protocolos de comunicación seguros. • Verificación de equipos mediante direcciones físicas, certificados, claves…
M11	Controles de seguridad para **almacén de claves criptográficas**	• Uso de TPM o elementos de hardware de almacenamiento seguro. • Despliegue de plataformas de autenticación centralizadas. • Almacenamientos *'en frío'* de claves criptográficas.
M12	Protección de **datos confidenciales en tránsito**	• Uso de protocolos con cifrado seguro. • Uso de VPN en caso de acceso interactivo.

M13	Medidas para la detección y recuperación de un ataque de **denegación de servicio**	• Bloqueo de cuentas y comunicaciones sospechosas repetidas. • Configuración de fallo seguro y de reinicio de comunicaciones. • Desplegar balanceadores de recursos.
M14	Protección ante **virus o *software* malicioso**	• Desplegar agentes de monitorización de *malware*. • Actualizar agentes periódicamente. • Implantar listas de *software* permitido para su instalación.
M15	Medidas para **detectar actividad o mensajes internos maliciosos**	• Desplegar agentes de monitorización y análisis de comunicaciones. • Recoger y analizar registros de actividad y comunicaciones en el vehículo. • Establecer un sistema de análisis y gestión de alertas de seguridad.
M16	Procedimientos **seguros de actualización de *software***	• Controles de integridad y autenticidad de *software* antes de su instalación. • Restringir acceso a la configuración del software. • Realizar copias de seguridad previas y posteriores a la actualización. • Diseñar un entorno de pruebas para verificar el funcionamiento de actualizaciones antes de su publicación. • Configuración de fallo seguro en caso de interrupción de la autenticación.
M18	Aplicar el **principio de mínimo privilegio** posible	• Definir roles y niveles de privilegios de usuarios según funciones y necesidades. • Habilitar registros de actividad de usuarios. • No habilitar cuentas privilegiadas por defecto
M19	Garantizar cumplimiento de **procedimientos de seguridad**	• Recopilación y análisis de registros de equipos. • Realizar ejercicios y jornadas de formación de ciberseguridad. • Establecer sistema de monitorización y análisis de alertas de seguridad.
M20	Controles de seguridad para **accesos remotos**	• Uso de protocolos de comunicación seguros. • Establecer control de accesos con múltiple factor de autenticación. • Restringir accesos remotos a orígenes reconocidos y autorizados. • Deshabilitar accesos remotos innecesarios.
M21	Se evaluará la **seguridad del *software***, se autenticará y se protegerá su integridad. Se aplicarán controles de seguridad para minimizar el riesgo procedente de software de terceros	• Establecer procesos de restauración de equipos. • Requerir privilegios elevados para la modificación de *software* y configuraciones. • Establecer *'listas blancas'* de software permitido.
M22	Controles de seguridad a las **interfaces externas**	• Requerir autenticación para acceder a interfaces externas. • Restringir comunicaciones externas solo para usos imprescindibles.

		• Mantener *software* y servicios accesibles desde el exterior actualizados.
M23	Se seguirán las mejores prácticas de ciberseguridad en el **desarrollo de *software* y *hardware***	• Mantener registros para la trazabilidad de funciones, versiones y capacidades de software. • Asegurar compatibilidad con medidas de seguridad. • Establecer y aplicar guías de bastionado.
M24	Se seguirán las mejores prácticas para la protección de la integridad y la confidencialidad de los **datos personales**	• Cifrado y monitorización de datos en reposo y en tránsito. • Segmentación de los sistemas que trabajan con datos confidenciales. • Notificar a los usuarios de la finalidad y metodología del uso de sus datos.

Además de implantar estas medidas de mitigación, la regulación estipula que el fabricante deberá **contar con los procesos y documentación** necesaria para asegurar que estas medidas funcionan debidamente. Para ello, la regulación estipula que los fabricantes deberán aplicar mitigaciones según los resultados de la gestión de riesgos, enfocando esfuerzos en los riesgos con mayor impacto potencial y probabilidad de afectar al vehículo y sus elementos críticos.

4.2.3. Mitigación de vulnerabilidades

Los fabricantes deberán gestionar y responder a las vulnerabilidades técnicas descubiertas en el software del vehículo en un plazo razonable.

Aunque este punto se desarrollará más adelante, cuando hablemos de la R156, para cumplir este objetivo, en esta guía se recomienda:

- Desplegar agentes de monitorización y detección de vulnerabilidades en el *software* del vehículo.
- Establecer canales de comunicación para que usuarios y terceros puedan notificar de nuevas vulnerabilidades descubiertas.
- Mantener un registro de las vulnerabilidades conocidas, nivel de impacto, características y estado de la gestión.
- Contar con un equipo de desarrollo de actualizaciones de seguridad para el *software* propio del fabricante y asegurarse de que los proveedores de *software* cuentan con capacidades equivalentes.
- Establecer un procedimiento para verificar el funcionamiento de las actualizaciones de seguridad antes de proporcionárselas a los usuarios.
- Notificar a los usuarios de las actualizaciones, su objetivo, los cambios aplicados e instrucciones para la actualización.

4.2.4. Análisis y detección de ciberamenazas

El fabricante deberá monitorizar los vehículos homologados, tras su venta, y de manera continua para detectar posibles amenazas.

Aunque la norma no específica metodología, cantidad ni tipología de datos a recoger de los vehículos vendidos por el fabricante, se considera que este requisito estipula la

necesidad de desplegar un sistema de administración de eventos e información de seguridad (SIEM) que monitorice, analice y notifique de la información de seguridad de los vehículos.
Es muy probable que la monitorización en tiempo real, solución estándar de los SIEM tradicionales, sea impracticable en el caso de vehículos, debido a las restricciones del producto: posible falta de cobertura o de desplazamientos a larga distancia, confidencialidad de los datos de los usuarios, longevidad del producto, uso de vehículos de segunda mano, etc.
Por tanto, se recomienda a los fabricantes diseñar sistemas para que los vehículos recolecten, local e independiente, los datos de seguridad pertinentes. Como mínimo, se recomienda la recolección de:

- Actividad de los usuarios y medidas de control de accesos.
- Conexiones establecidas entre sistemas del vehículo y con sistemas externos.
- Cambios en *software* y *hardware.*
- Actividad inusual o potencialmente peligrosa para la seguridad del vehículo.
- Actividad de las medidas de seguridad instaladas, como agentes *antimalware* o de control de comunicaciones.

Los datos deberían suministrar al SIEM de manera periódica para su análisis, o cuando el vehículo vuelva a tener conectividad.

Será responsabilidad del fabricante velar por la confidencialidad y seguridad de los usuarios del vehículo.

Durante la aplicación de este requisito, independientemente de la metodología usada, se deberá **informar al usuario de la recopilación de datos y su finalidad**. También se deberá asegurar que las **funciones de monitorización no tienen un impacto negativo en la funcionalidad del vehículo**. Se recomienda priorizar las soluciones de monitorización pasivas y no intrusivas en los sistemas del vehículo, que minimicen su efecto en los sistemas del vehículo.

4.2.5. Dependencias con proveedores contratados

Los fabricantes mantengan una correcta gestión de la ciberseguridad a lo largo de la cadena de suministro.

Se recomienda que, durante el análisis de riesgo realizado en la etapa de diseño, el fabricante identifique qué partes del vehículo van a ser provistas por terceros y qué características de seguridad deberían incluir. Estas características deberían ser requisitos que presentar a los proveedores en el momento de contratación de sus servicios y debería la capacidad para cumplirlos debería ser un criterio a la hora de seleccionar proveedores.
A nivel de evidencia, el fabricante podría solicitar a los proveedores: certificaciones de seguridad de su equipo, resultados de pruebas técnicas, especificaciones técnicas del producto, compromisos legales de cumplimiento de requisitos.
Entre los aspectos más comunes a definir en los requisitos con los proveedores en materia de ciberseguridad, se podría encontrar:

- Responsabilidades de soporte técnico y actualizaciones de seguridad para el software y hardware provisto, y duración de este servicio.
- Responsabilidades de apoyo del proveedor durante la respuesta ante incidentes.
- Canales de comunicación para notificaciones de ciberseguridad.

- Guías de bastionado e instrucciones de seguridad para el equipo provisto.
- Accesos remotos del proveedor y accesos a información sensible del fabricante y de los usuarios finales del vehículo.
- Compatibilidad con las medidas de seguridad utilizadas por el fabricante y aplicabilidad de los procedimientos y políticas de este en el equipo provisto (política de contraseñas, compatibilidad con los agentes antimalware y de monitorización…).
- Aprovisionamiento de repuestos y reemplazos.

4.3. Requisitos para cada tipo de vehículo homologado

Además de los requisitos para el SGSI del fabricante, la R155 estipula una serie de requisitos relativos a la seguridad desplegada en el propio vehículo.

La homologación se solicita y se otorga para cada tipo de vehículo de manera independiente.
Los requisitos anteriores, en gran parte, pueden ser cumplidos por el fabricante para todos los tipos de vehículos en producción a la vez (por ejemplo, un procedimiento interno del fabricante para el desarrollo seguro de software se aplicará a todos los tipos de vehículos con los que se esté trabajando mientras se sigue el procedimiento). Sin embargo, los siguientes requisitos se deben cumplir de manera independiente para cada tipo de vehículo.

4.3.1. Cumplimiento de todos los requisitos del SGSI

El fabricante deberá certificar que el tipo de vehículo a homologar es compatible con su SGSI y se cumplen todos los requisitos estipulados para este.

Para evidenciar este cumplimiento el fabricante deberá emitir una declaración de conformidad siguiendo la plantilla recogida en los anexos de la regulación R155 (Figura 3).

Esta declaración acompañaría a la ficha técnica (Figura 2) en el momento de solicitud de la homologación y debe emitirse tras pasar las pruebas técnicas internas del fabricante requeridas por la regulación para verificar que el SGSI cumple sus funciones correctamente.

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*)

Figura 3: Declaración de conformidad del SGSI

Para los vehículos de nueva fabricación, este requisito no debería presentar mucha dificultad si se ha realizado correctamente la gestión del riesgo durante el diseño y producción.
Para modelos antiguos no compatibles, como contempla la regulación, el fabricante puede realizar un análisis de riesgos sobre el tipo de vehículo. El fabricante deberá certificar, mediante el análisis de riesgos, y potencialmente mediante el despliegue de nuevas medidas con carácter retroactivo, que presenta un nivel de ciberseguridad adecuado pese a no ser compatible con el SGSI.

4.3.2. riesgos relativos a los proveedores

El fabricante deberá determinar y gestionar los riesgos relacionados con el proveedor para el tipo de vehículo sujeto a homologación.

Igual que el punto anterior, este requisito debería cumplirse automáticamente si el fabricante está aplicando su SGSI para el tipo de vehículo en las fases de diseño y producción. Este requisito remarca la necesidad no utilizar requisitos y análisis genéricos para cada tipo de vehículo, es necesario asegurar que en cada caso se cumplen las necesidades concretas del producto y proceso a homologar.

4.3.3. Elementos críticos del vehículo

El fabricante deberá Identificar los elementos críticos del vehículo y realizar una evaluación de riesgo sobre ellos.

Se deberían considerar críticos aquellos elementos que puedan afectar a los elementos esenciales del vehículo, aquellos que, en caso de interrumpirse su servicio la funcionalidad del vehículo y la seguridad de los pasajeros se pueda ver comprometida.
En general, estos elementos deberían encontrarse aislados lo máximo posible del resto de sistemas del vehículo. Los canales de comunicación establecidos con los elementos

críticos deberían contar con el máximo nivel de seguridad posible y solamente deberían establecerse en caso de necesidad. Esta precaución deberá extremarse para el caso de conexiones con redes externas. Estas deberán restringirse lo máximo posible en el caso de elementos críticos del vehículo, habilitándose solo en caso de ser imprescindibles para el funcionamiento de vehículo, con las máximas medidas de seguridad posible e, idealmente, mediante sistemas que actúen de intermediarios, por ejemplo, mediante redes de separación.

4.3.4. Medidas de seguridad del vehículo

Requisitos	Comentarios
Certificar que el tipo de vehículo a homologar cuenta con las **medidas de mitigación** correspondientes desplegadas, según el análisis de riesgos realizado	Realizar una gestión sistemática de la seguridad, identificando y priorizando riesgos y siguiendo las medidas de mitigación de la regulación descritas anteriormente.
Garantizar que el tipo de vehículo cuenta con un **entorno seguro para el almacenaje y ejecución de *software***	◻ Establecer un entorno aislado del resto de servicios de *software.* ◻ Contar con un control de versiones. ◻ Monitorizar la integridad del *software* almacenado. ◻ Restringir el acceso y los permisos de ejecución y modificación, reservándolo para aquellos casos donde sea imprescindible para la funcionalidad y seguridad del vehículo. ◻ Mantener registros de ejecuciones y modificaciones de *software* para mantener la trazabilidad sobre el *software*. ◻ Implementar listas de *software* autorizado para la ejecución.
En el vehículo existen medidas técnicas de seguridad para garantizar que el ***software* y los servicios instalados se ejecutan de manera segura**	
Las medidas de seguridad del vehículo han sido probadas para verificar su funcionamiento y eficacia.	No se especifican la tipología de pruebas a realizar, pero se puede acudir a estándares reconocidos como las ISO/SAE 21434, ISO 26262-2018 e ISO/PAS21448 para obtener una idea de buenas prácticas a seguir en las pruebas.
Someter el tipo de vehículo a homologar a **ensayos adecuados y suficientes para verificar la eficacia de las medidas de seguridad** aplicadas.	
El vehículo, durante su vida útil, proporciona información al fabricante para que este pueda identificar, gestionar y analizar posibles amenazas (sin comprometer la privacidad de los usuarios).	El fabricante debería identificar posibles puntos de conexión seguros para el envío de *logs* de seguridad. Una posibilidad sería utilizar la conexión del móvil del usuario mediante aplicaciones como Android Auto y Apple Carplay o aplicaciones propias. En caso de uno usar conexiones inalámbricas, el proceso deberá apoyarse en los servicios técnicos autorizados
Evidenciar que el tipo de vehículo cuenta con **capacidades forenses** en cuanto a ciberincidentes: recogida de	

registros de las medidas de seguridad y el software del vehículo, los registros están protegidos frente a alteraciones no autorizadas y son evaluados periódicamente para detectar ciberincidentes.	
El vehículo cuenta con sistemas criptográficos suficientes para cumplir con la regulación de privacidad vigente.	La criptografía no debería aplicarse solo a las comunicaciones remotas del vehículo. Se recomendaría su aplicación sobre las bases de datos internas, sobre todo en aquellos casos donde se almacena datos del usuario o de seguridad. Una metodología sería el uso de sistemas equivalentes a los TPM utilizados hoy en día en otros sectores para cifrar equipos a nivel de *hardware*.
El fabricante notificará, al menos anualmente, de los **resultados de la gestión de la ciberseguridad** (incluyendo información sobre nuevas ciberamenazas y ciberataques).	Estos requisitos pueden servir de motivación para que el fabricante centralice la información y mantenga una gestión eficiente. Es habitual generar informes mensuales (o incluso semanales) del estado de la ciberseguridad en un sistema de control industrial. En estos informes se suele incluir: ▫ Estado de las vulnerabilidades conocidas y sus medidas de mitigación. ▫ Eventos e incidentes de ciberseguridad gestionados. ▫ Nuevas amenazas descubiertas mediante monitorización de los sistemas o fuentes públicas. ▫ Avances en los planes de acción de ciberseguridad. A la hora de hacer modificaciones, igual que en la fase de diseño, es importante tener visión de como afectarán a las medidas de seguridad. Para ello es habitual servirse de nuevos análisis de riesgos o pruebas técnicas, antes de decidir si se necesitan medidas adicionales.
El fabricante deberá **notificar a la autoridad homologadora de todas las modificaciones** que afecten al rendimiento de las medidas de ciberseguridad o a la documentación presentada previamente.	

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

5. R156: Actualización de software

Igual que para la regulación R155, la R156 define un formulario de información que el fabricante debe proporcionar para optar a la homologación. (Figura 4).

Ficha de características

La información que figura a continuación deberá presentarse, en su caso, por triplicado e ir acompañada de un índice de contenidos. Todos los dibujos se entregarán a la escala adecuada, tendrán un nivel de detalle suficiente y se presentarán en formato A4 o plegados de forma que se ajusten a ese formato. Si se presentan fotografías, deberán ser suficientemente detalladas.

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

2. Tipo y denominaciones comerciales generales: .....

   (El tipo se refiere al tipo que va a homologarse, la denominación comercial se refiere al producto en el que se utiliza el tipo homologado)

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

4. Emplazamiento de dicho marcado: .....

5. Categoría o categorías del vehículo: .....

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

7. Nombres y direcciones de las plantas de montaje: .....

8. Fotografías o planos de un vehículo representativo: .....

9. Actualizaciones de *software*

9.1. Características generales de fabricación del tipo de vehículo: .....

9.2. Número del certificado de conformidad del sistema de gestión de actualizaciones de *software*: .....

9.3. Medidas de seguridad.

9.3.1. Documentos relativos al tipo de vehículo que va a homologarse en los que se describe que el proceso de actualización se realizará de forma segura .....

9.3.2. Documentos relativos al tipo de vehículo que va a homologarse en los que se describe que los identificadores RXSWIN de un vehículo están protegidos contra la manipulación no autorizada. .....

9.4. Actualizaciones de *software* por aire

9.4.1. Documentos relativos al tipo de vehículo que va a homologarse en los que se describe que el proceso de actualización se realizará de forma segura .....

9.4.2. De qué modo se podrá informar al usuario del vehículo sobre una actualización antes y después de su ejecución .....

Figura 4: Anexo 1 de la regulación R156. Información a aportar por el fabricante

En este caso, la homologación se centra en la ciberseguridad del *software* del vehículo y su mantenimiento durante el ciclo de vida de este. la regulación estipula que los fabricantes deberán implementar un sistema para asegurar que se desarrollan actualizaciones de seguridad del *software* alojado en el vehículo y que estas se distribuyen y aplican sin introducir nuevos riesgos para el vehículo y sus ocupantes.
Igual que en el caso de la R155, los fabricantes deben garantizar que han cumplidos los requisitos mediante otro formulario (Figura 5).

Modelo de declaración de la conformidad del sistema de gestión de actualizaciones de *software*

Declaración de conformidad del fabricante con los requisitos del sistema de gestión de actualizaciones de *software*

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 relativos al sistema de gestión de actualizaciones de *software* establecidos en el punto 7.1 del Reglamento n.º 156 de Naciones Unidas.

Hecho en: ..... (lugar)

Fecha: .....

Nombre del firmante: .....

Cargo del firmante: .....

.....

(Sello y firma del representante del fabricante)

Figura 5: Declaración de conformidad del sistema de gestión de actualizaciones de software

5.1. Requisitos del sistema de gestión de actualizaciones de software.

5.1.1. A cumplir en el momento de la evaluación inicial

La regulación estipula la necesidad de que el fabricante establezca **procesos** para cumplir los siguientes requisitos:

Requisitos	Comentarios y recomendaciones
Se documenta y se conserva toda la información, relativa al ***software*** del vehículo, pertinente para el cumplimiento de la regulación	La información a recopilar se amplía con más detalle en el siguiente apartado.
Existe un **método para identificar de manera unívoca todas las versiones** del *software* y actualizaciones desplegadas	Los indicadores son a selección del fabricante, pero es importante que se documenten y sean consistentes. El identificador RXSWIN es un número, seleccionado por el fabricante, que identifica el *software* del sistema electrónico de control del tipo de vehículo homologado. La X del código representa el reglamento al que hace referencia el identificador, en este caso R156WIN.
Para los vehículos que tengan un identificador **RXSWIN**, la información relativa al identificador RXSWIN antes y después de la actualización está accesible y puede actualizarse.	

El fabricante puede verificar que **el *software* se ajusta a lo definido por el identificador**	◻ Definir firmas de *software* y listas de *software* autorizado y guías sobre como identificarlo. ◻ De manera adicional, añadir medidas de seguridad adicionales para monitorizar la integridad del *software* y restringir el acceso y modificación
Identificar todas las **interdependencias del sistema actualizado con otros sistemas**	En el caso del *software* de los componentes, las interdependencias pueden darse principalmente en forma de: ◻ Otros paquetes de *software* externos que se necesitan para funcionar debidamente; ◻ Conexiones que el *software* actualizado necesita establecer con otros sistemas para realizar sus funciones; ◻ Información alojada externamente a la que el *software* actualizado necesita acceso.
Evaluar, determinar y registrar si una actualización podría afectar a otros sistemas necesarios para el funcionamiento seguro del vehículo, o si alterará las funciones de este respecto al momento de su matriculación	Aunque siempre se recomienda la realización de pruebas técnicas antes de publicar la actualización, una correcta gestión de la ciberseguridad permite identificar puntos de interacción entre sistemas mediante inventarios, análisis de riesgos y monitorización.
Identificar todos los vehículos objetivo para la actualización. Refiriéndose a los vehículos, en producción o en postproducción, en los que está desplegado el *software* a actualizar	Este requisito infiere la necesidad de mantener inventarios actualizados de los vehículos en funcionamiento con la versión del *software* a actualizar y recoger una mínima relativa al *software* y sistemas instalados
Confirmar la compatibilidad de la actualización con la configuración de los vehículos objetivos antes de su lanzamiento.	Pese a que la compatibilidad puede determinarse de manera formal por las especificaciones de la actualización, se recomienda contar con entornos de prueba y verificar las actualizaciones.
Evaluar, determinar y registrar si una actualización afectará a cualquier sistema homologado.	Es importante remarcar, que una actualización que altere fundamentalmente alguno de los componentes homologados puede conllevar la necesidad de renovar esta homologación, requiriendo pruebas o información adicional antes de que vuelva a aprobarse
Informar al usuario de las actualizaciones	Informar de: ◻ objetivo de la actualización, ◻ instrucciones a seguir, ◻ cambios que se van a realizar, ◻ progreso de la actualización, ◻ éxito o fallo del proceso.

5.1.2. Información a registrar y almacenar

Para cada actualización, el fabricante deberá registrar y almacenar:

- Documentación de los procesos utilizados para el desarrollo de las actualizaciones.
- Documentación de la composición e identificadores de los sistemas homologados antes y después de la actualización.
- Los dos siguientes puntos, además de almacenarse, también **deberán presentarse en el momento de la homologación**:
  - Para cada RXSWIN, un registro comprobable de su composición antes y después de la actualización.
  - Documentación que enumere los vehículos objetivo de la actualización y confirmación de la compatibilidad respecto a la última configuración de estos
- Documentación de cada actualización:
  - objetivo,
  - sistemas afectados y cuáles han sido homologados,
  - si afecta a otros requisitos,
  - si afecta a parámetros de homologación de algún sistema,
  - si se ha solicitado su homologación,
  - cómo y cuándo se puede aplicar la actualización,
  - confirmación de que la actualización es segura,
  - confirmación de que se ha sometido a procedimientos de validación de manera satisfactoria.

Como se puede observar, la mayoría de esta información podría recopilarse a la vez que se cumplen los requisitos solicitados para el momento inicial de la homologación. Esto pone énfasis en la necesidad de contar con una gestión que permita cumplir estos requisitos de manera sistemática para cada actualización.

5.1.3. Requisitos adicionales de seguridad

El fabricante deberá demostrar que:

- **Las actualizaciones están protegidas ante manipulación no autorizada**, antes de proceder a la actualización.
- **El proceso de actualización está protegido**, incluido el suministro de la actualización a los vehículos objetivos.

El cifrado de comunicaciones, aplicación de controles de integridad y autenticación y el diseño de arquitecturas seguras, son particularmente críticas para proteger las actualizaciones de seguridad en tránsito y prevenir la manipulación inadecuada del *software* del vehículo.
Pero también es importante tener en cuenta otras cuestiones, como la composición de la red. Para una mayor seguridad, se pueden utilizar comunicaciones unidireccionales, no interactivas, a través de elementos intermedios de protección o, en última instancia, recurrir a soportes físicos en talleres especializados para la información crítica.

5.1.4. Requisitos adicionales para actualizaciones inalámbricas

El fabricante deberá tener en cuenta los siguientes requisitos a la hora de elegir la metodología de actualización de vehículos a seguir:

- Demostrar que los **procesos de actualización no afectan a la seguridad** durante la conducción.

- Demostrar que, en caso de que la **actualización requiera acciones especializadas** o complejas, la aplicación solo puede aplicarse en presencia de personal competente.

Es posible que las actualizaciones más sencillas puedan realizarse de manera inalámbrica y simultánea a todos los vehículos objetivos. Sin embargo, pese a la incomodidad que supone para el usuario, conviene considerar solicitar que lleven sus vehículos a servicios técnicos preparados para actualizaciones críticas o más técnicas. Es importante dotar a los talleres con guías de actualización y credenciales con suficiente nivel de privilegios para que puedan realizar esta tarea. El momento de actualización presencial también puede ser una oportunidad para la recopilación de datos de seguridad de locales del vehículo para su análisis.

- El vehículo deberá ser capaz de:
  - Restaurar sus sistemas a una versión anterior en caso de interrupción o fallo de la actualización.
    - Se deberá valorar la posibilidad de almacenar las copias de seguridad para la restauración del sistema directamente en el vehículo, frente al uso de servidores externos. Esta decisión condicionará la capacidad de almacenamiento en el vehículo, almacenamiento que deberá estar protegido y monitorizado, con controles de integridad y autenticación.
      El uso de servidores externos, en cambio, introduce riesgos de disponibilidad y confidencialidad. Estos riesgos se multiplican en el caso de vehículos en movimiento o en zonas remotas que pueden perder la conectividad.
  - Entrar en un estado de fallo seguro en caso de interrupción o fallo de la actualización.
    - En ningún caso el vehículo debería interrumpir su servicio o comprometer la seguridad física de los usuarios en caso de fallo durante el proceso de actualización. Aunque el método más seguro es realizar las actualizaciones solamente cuando el vehículo esté detenido, es posible que esta decisión comprometa la capacidad de batería del vehículo o su disponibilidad, si el proceso de actualización es largo.
  - No permitir iniciar un proceso de actualización a no ser que el vehículo cuente con la potencia suficiente para completar el proceso.
    - Durante las pruebas de verificación de la actualización, el fabricante puede obtener una estimación del consumo de batería necesario para completar el proceso, y aplicarla como límite de seguridad para el proceso. Alternativamente, se podría establecer un límite de seguridad general para no iniciar procesos con batería baja, como se realiza de manera estándar en otros dispositivos electrónicos móviles.
  - Contar con un proceso seguro para actualizaciones que afecten la seguridad del vehículo.
    - Se recomienda que las actualizaciones que afecten la seguridad del vehículo se realicen cuando este esté detenido y bajo confirmación

de un usuario autenticado, o el personal técnico especializado si es necesario.

- El fabricante deberá poder informar al usuario de una actualización antes de que esta se ejecute. Deberá informar de:
  - Propósito de la actualización.
    - Se deja de manera opcional si el fabricante notifica de la criticidad y tipo de actualización.
  - Cambios introducidos por la actualización.
  - Tiempo previsto para completar la actualización.
  - Funciones que puedan estar no disponibles durante el proceso. Instrucciones que el usuario pueda necesitar para actualizar el vehículo de manera segura.
  - **Se aceptará una** misma **notificación** para un grupo de actualizaciones que se vayan a aplicar de manera consecutiva.
- En los casos donde la actualización no sea segura durante la conducción, se garantizará que el vehículo no permite la conducción durante la actualización (o viceversa), ni el uso de funciones que puedan comprometer el proceso o la seguridad del vehículo.
- Tras la actualización del vehículo se informará al usuario del éxito o fracaso del proceso y de los cambios aplicados.

6. Conclusiones

Las nuevas regulaciones de ciberseguridad para vehículos representan un cambio significativo en los procesos habituales de los fabricantes, que ahora se deberán enfrentar al desafío de proporcionar protección a múltiples sistemas en constante movimiento sin comprometer la seguridad física de los usuarios o la funcionalidad de los vehículos.

Aunque la mayoría de los nuevos requisitos de ciberseguridad se podrán cumplir fácilmente si se aplica un sistema integral de gestión de la ciberseguridad a nivel de la empresa del fabricante: estableciendo procedimientos internos de ciberseguridad, realizando análisis de riesgos y estableciendo requisitos y controles de ciberseguridad a lo largo de la cadena de suministro; existen algunos casos concretos que presentan un nivel de dificultad mayor.

Los requisitos relacionados con la fase de mantenimiento del vehículo, cuando este está en uso por el cliente final, pueden requerir especial atención. ¿Qué información debe registrar el coche durante su uso? ¿Cómo va a llegar la información al fabricante para su análisis y cada cuánto? ¿Cómo se van a suministrar las actualizaciones?

Para muchos de estos procesos las soluciones más cómodas para el fabricante no serán la mejor opción para el usuario final. Por ejemplo, un fabricante puede optar por requerir que el cliente lleve el vehículo periódicamente al servicio técnico como método único para aplicar actualizaciones de ciberseguridad, lo que conllevaría costes adicionales y molestias para el cliente.

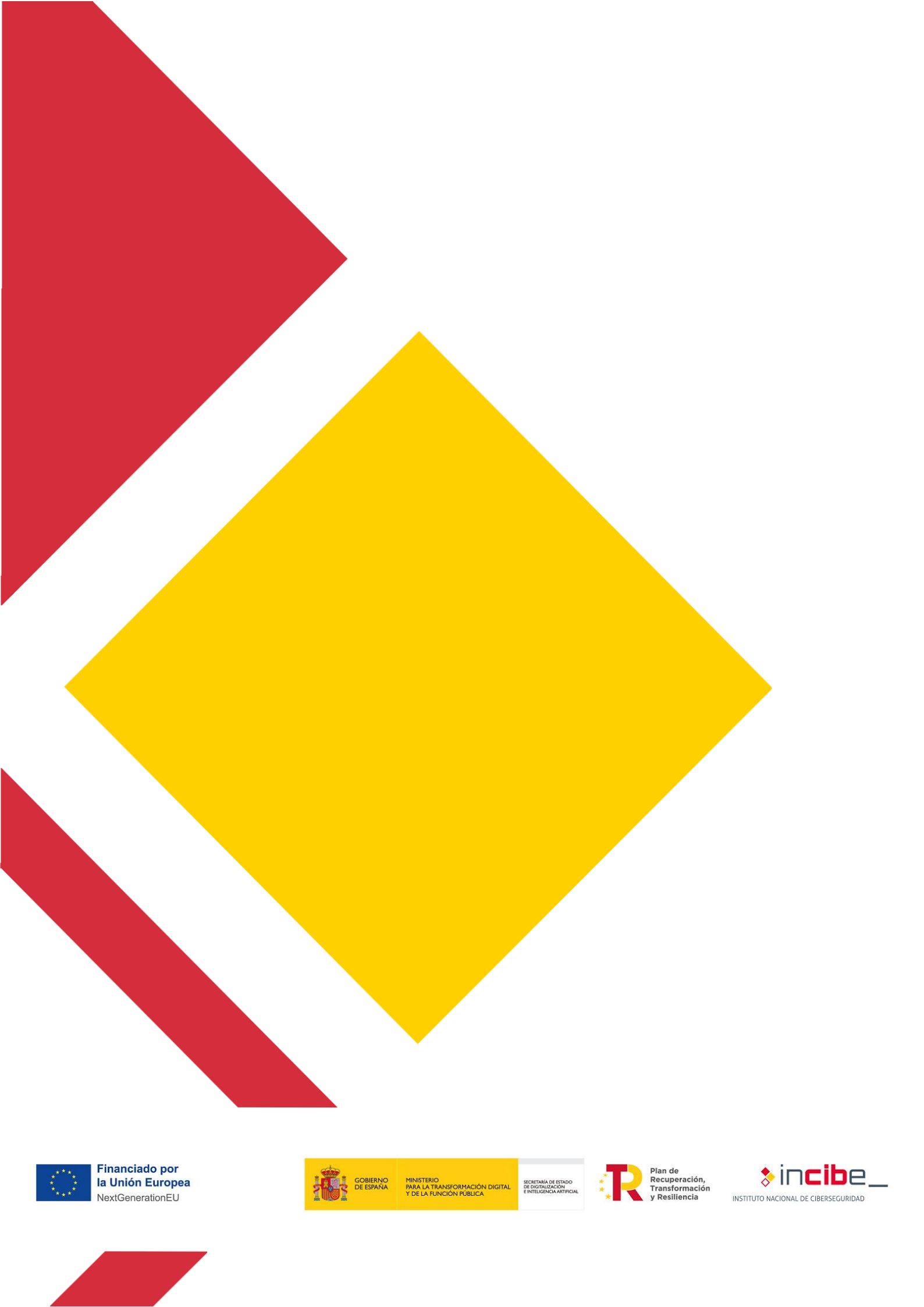
Sin embargo, los procesos más avanzados y con mayor funcionalidad requerirán tenerse en cuenta desde el momento de diseño de nuevos vehículos, o incurrir en mayores costes a la hora de aplicarse retroactivamente.

Como ya se ha comentado a lo largo del presente documento, e ilustra este último ejemplo, la ciberseguridad debe tratarse de manera global en la empresa. Cada paso del proceso es una pieza base para la siguiente etapa que ayudará a la efectividad de las medidas de seguridad, el cumplimiento de la nueva regulación y la reducción de impacto y recursos necesarios para la gestión de incidentes.

ANEXO I. Glosario de términos

Término	Definición
Software	Programas o servicios instalados en un equipo para realizar las funcionalidades objetivo
Hardware	Componentes físicos de un equipo que alojan que realizan tareas por si mismos o alojan el *software* para su ejecución.
Sistema de gestión de la ciberseguridad (SGSI)	Conjunto de políticas, procedimientos, medidas y controles implementados en una organización para cumplir los objetivos de ciberseguridad.
Vulnerabilidad	Deficiencia o debilidad técnica de un *software* o *hardware* que introduce un riesgo de ciberseguridad para un equipo.
Tipo de vehículo	Conjuntos de vehículos que comparten: • La misma designación definida por el fabricante. Mismo nombre o número de modelo elegido por el fabricante. • Las mismas características esenciales de la arquitectura eléctrica y electrónica y las interfaces externas, en lo que respecta a la ciberseguridad.
Actualización o parche de seguridad	Nueva versión de un *software* que introduce cambios en su configuración para eliminar vulnerabilidades.
Trusted Platform Machine (TPM)	*Hardware* dedicado al almacenamiento de claves de cifrado de un equipo para proteger información confidencial o la configuración de un equipo.

.


Financiado por
la Unión Europea
NextGenerationEU
GOBIERNO
DE ESPAÑA
MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL
Plan de
Recuperación,
Transformación
y Resiliencia
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD