Só os textos originais da UNECE fazem fé ao abrigo do direito internacional público. O estatuto e a data de entrada em vigor do presente regulamento devem ser verificados na versão mais recente do documento UNECE comprovativo do seu estatuto, TRANS/WP.29/343, disponível em: https://unece.org/status-1958-agreement-and-annexed-regulations

Regulamento n.º 155 da ONU — Prescrições uniformes relativas à homologação de veículos no que diz respeito à cibersegurança e ao sistema de gestão da cibersegurança [2025/5]

Integra todo o texto válido até:

Suplemento 3 à versão original do regulamento — Data de entrada em vigor: 10 de janeiro de 2025

O presente documento constitui apenas um instrumento documental. Os textos que fazem fé e são juridicamente vinculativos são os seguintes:

— ECE/TRANS/WP.29/2020/79 (alterado por ECE/TRANS/WP.29/2020/94 e ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 e

— ECE/TRANS/WP.29/2024/55

ÍNDICE

Regulamento

1. Âmbito de aplicação
2. Definições
3. Pedido de homologação
4. Marcações
5. Homologação
6. Certificado de conformidade do sistema de gestão da cibersegurança
7. Especificações
8. Modificação do modelo de veículo e extensão da homologação
9. Conformidade da produção
10. Sanções por não conformidade da produção
11. Cessação definitiva da produção
12. Designações e endereços dos serviços técnicos responsáveis pela realização dos ensaios de homologação e das entidades homologadoras

Anexos

1 Ficha de informações

2 Comunicação

3 Exemplo de marca de homologação

4 Modelo de certificado de conformidade do CSMS

5 Lista de ameaças e respetivas medidas de mitigação

1. Âmbito de aplicação

1.1. O presente regulamento aplica-se aos veículos das categorias L, M, N e O no que diz respeito à cibersegurança se estiverem equipados com, pelo menos, uma unidade de controlo eletrónico.

1.2. O presente regulamento não prejudica os outros regulamentos da ONU, as legislações regionais ou nacionais que regem o acesso das partes autorizadas ao veículo e aos seus dados, funções e recursos, bem como as respetivas condições de acesso. Também não prejudica a aplicação da legislação nacional e regional relativa à privacidade e à proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais.

1.3. O presente regulamento aplica-se sem prejuízo de outros regulamentos da ONU, da legislação nacional ou regional que rege a conceção e a instalação ou integração de peças e componentes de substituição, físicas e digitais, no que diz respeito à cibersegurança.

2. Definições

Para efeitos do presente regulamento, entende-se por:

2.1. «*Modelo de veículo*», o conjunto de veículos que não diferem entre si, pelo menos, nos seguintes aspetos essenciais:

a) A designação do modelo de veículo pelo fabricante;

b) Os aspetos essenciais da arquitetura elétrica/eletrónica e das interfaces externas no que respeita à cibersegurança.

2.2. «*Cibersegurança*», a proteção dos veículos rodoviários e das suas funções contra ciberameaças a componentes elétricos ou eletrónicos.

2.3. «*Sistema de gestão da cibersegurança (CSMS)*», uma abordagem sistemática baseada nos riscos e que define os processos organizacionais, as responsabilidades e a governação para tratar os riscos associados às ciberameaças aos veículos e protegê-los contra ciberataques.

2.4. «*Sistema*», um conjunto de componentes e/ou subsistemas que executa uma ou mais funções.

2.5. «*Fase de desenvolvimento*», o período que antecede a homologação de um modelo de veículo.

2.6. «*Fase de produção*», a duração da produção de um modelo de veículo.

2.7. «*Fase de pós-produção*», o período em que um modelo de veículo deixou de ser produzido até ao fim da vida útil de todos os veículos deste modelo. Os veículos conformes a um modelo de veículo específico continuam operacionais durante esta fase, mas já não são produzidos. A fase termina quando já não existem veículos operacionais de um modelo de veículo específico.

2.8. «*Medida de mitigação*», uma medida que reduz os riscos.

2.9. «*Risco*», a possibilidade de que uma determinada ameaça explore as vulnerabilidades de um veículo e cause assim danos à organização ou a um indivíduo.

2.10. «*Avaliação dos riscos*», o processo global de verificação, reconhecimento e descrição dos riscos (identificação dos riscos), para compreensão da natureza do risco e determinação do nível de risco (análise dos riscos), assim como da comparação dos resultados da análise dos riscos com critérios de risco para determinar se os riscos e/ou a sua magnitude são aceitáveis ou toleráveis (avaliação dos riscos).

2.11. «*Gestão dos riscos*», as atividades coordenadas para dirigir e controlar uma organização em matéria de riscos.

2.12. «*Ameaça*», uma causa potencial de um incidente indesejável que pode resultar em danos para um sistema, uma organização ou um indivíduo.

2.13. «*Vulnerabilidade*», insuficiência de um elemento ou de uma medida de mitigação que possa ser explorada por uma ou mais ameaças.

3. Pedido de homologação

3.1. O pedido de homologação de um modelo de veículo no que diz respeito à cibersegurança deve ser apresentado pelo fabricante do veículo ou pelo seu representante devidamente acreditado.

3.2. O pedido deve ser acompanhado pelos documentos a seguir mencionados, em triplicado, e pelo seguinte:

3.2.1. Uma descrição do modelo de veículo no que diz respeito aos elementos especificados no anexo 1 do presente regulamento;

3.2.2. Nos casos em que se mostre ser a informação abrangida por direitos de propriedade intelectual ou constituir um saber-fazer específico do fabricante ou dos seus fornecedores, o fabricante ou os seus fornecedores devem disponibilizar informações suficientes para permitir a realização correta dos controlos referidos no presente regulamento. Essas informações devem ser tratadas confidencialmente;

3.2.3. O certificado de conformidade do CSMS, em conformidade com o ponto 6 do presente regulamento.

3.3. A documentação deve ser disponibilizada em duas partes:

a) O dossiê oficial de documentação para homologação, com os materiais especificados no anexo 1, que deve ser fornecido à entidade homologadora ou ao seu serviço técnico aquando da apresentação do pedido de homologação. O dossiê de documentação deve ser utilizado pela entidade homologadora ou pelo seu serviço técnico como referência de base para o processo de homologação. A entidade homologadora ou o seu serviço técnico devem assegurar que este dossiê de documentação esteja disponível durante, pelo menos, 10 anos a partir da data em que a produção do modelo de veículo cessou de forma definitiva.

b) O material adicional relevante para os requisitos do presente regulamento pode ser conservado pelo fabricante, mas deve ser colocado à disposição para inspeção aquando da homologação. O fabricante deve assegurar que qualquer material facultado para efeitos de inspeção aquando da homologação permanece disponível durante um período de, pelo menos, 10 anos a partir da data em que a produção do modelo de veículo cessou de forma definitiva.

4. Marcação

4.1. Nos veículos conformes a modelos de veículos homologados nos termos do presente regulamento, deve ser afixada de maneira visível, num local facilmente acessível e indicado na ficha de homologação, uma marca de homologação internacional composta por:

4.1.1. Uma circunferência envolvendo a letra «E» seguida do número distintivo do país que concedeu a homologação;

4.1.2. O número do presente regulamento, seguido da letra «R», de um travessão e do número de homologação, colocados à direita da circunferência descrita no ponto 4.1.1.

4.2. Se o veículo for conforme a um modelo de veículo homologado, nos termos de um ou mais dos regulamentos anexados ao Acordo, no país que concedeu a homologação de acordo com o presente regulamento, o símbolo previsto no ponto 4.1.1 não tem de ser repetido; neste caso, os números do regulamento e da homologação e os símbolos adicionais de todos os regulamentos ao abrigo dos quais tiver sido concedida a homologação no país em causa em aplicação do presente regulamento serão dispostos em colunas verticais à direita do símbolo prescrito no ponto 4.1.1.

4.3. A marca de homologação deve ser claramente legível e indelével.

4.4. A marca de homologação deve ser colocada sobre a chapa de identificação do veículo afixada pelo fabricante, ou na sua proximidade.

4.5. O anexo 3 do presente regulamento dá exemplos da disposição das marcas de homologação.

5. Homologação

5.1. As entidades homologadoras concedem, conforme adequado, a homologação no que diz respeito à cibersegurança, apenas aos modelos de veículos que cumpram os requisitos do presente regulamento.

5.1.1. A entidade homologadora ou o seu serviço técnico devem verificar os documentos que atestam que o fabricante do veículo tomou as medidas necessárias em função do modelo de veículo, para:

a) Recolher e verificar, ao longo da cadeia de abastecimento, as informações exigidas pelo presente regulamento, de modo a demonstrar que os riscos relacionados com os fornecedores são identificados e são geridos;

b) Documentar a avaliação dos riscos (realizada durante a fase de desenvolvimento ou retrospetivamente), os resultados dos ensaios efetuados e as medidas de mitigação aplicadas ao modelo de veículo, incluindo informações sobre a conceção que apoiem a avaliação dos riscos;

c) Aplicar medidas adequadas de cibersegurança na conceção do modelo de veículo;

d) Detetar as ameaças e reagir a possíveis ciberataques;

e) Registar dados para apoiar a deteção de ciberataques e dispor de capacidade de investigação forense de dados que permitam a análise de ciberataques tentados ou consumados.

5.1.2. A entidade homologadora ou o seu serviço técnico devem verificar, através de ensaios a um veículo do modelo do veículo, que o fabricante aplicou as medidas de cibersegurança que documentou. Os ensaios devem ser realizados pela própria entidade homologadora ou pelo seu próprio serviço técnico ou em colaboração com o fabricante do veículo por amostragem. A amostragem deve focar-se, mas não incidir exclusivamente, nos riscos considerados elevados durante a avaliação dos riscos.

5.1.3. A entidade homologadora ou o seu serviço técnico devem recusar a homologação no que diz respeito à cibersegurança se o fabricante do veículo não tiver cumprido um ou mais dos requisitos referidos no ponto 7.3, nomeadamente:

a) Se o fabricante do veículo não tiver efetuado a avaliação exaustiva dos riscos referida no ponto 7.3.3; incluindo nos casos em que o fabricante não tenha tomado em consideração todos os riscos relacionados com as ameaças referidas no anexo 5, parte A;

b) Se o fabricante do veículo não tiver protegido o modelo de veículo contra os riscos identificados na avaliação dos riscos por si realizada ou não tiverem sido aplicadas medidas de mitigação proporcionadas, tal como exigido no ponto 7;

c) Se o fabricante do veículo não tiver posto em prática medidas adequadas e proporcionadas para garantir a segurança de ambientes específicos no modelo de veículo (se fornecidos) para o armazenamento e a execução de *software*, serviços, aplicações ou dados pós-venda;

d) Se o fabricante do veículo não tiver efetuado, antes da homologação, ensaios adequados e suficientes para verificar a eficácia das medidas de segurança aplicadas.

5.1.4. A entidade homologadora encarregada da avaliação deve também recusar a homologação no que diz respeito à cibersegurança se nem ela nem o seu serviço técnico tiverem recebido do fabricante informações suficientes para avaliar a cibersegurança do modelo de veículo.

5.2. A comunicação da concessão, extensão ou recusa da homologação de um modelo de veículo nos termos do presente regulamento deve ser feita às partes no Acordo de 1958 que apliquem o presente regulamento através de um formulário conforme com o modelo apresentado no anexo 2 do presente regulamento.

5.3. As entidades homologadoras não devem conceder qualquer homologação sem verificar se o fabricante pôs em prática disposições e procedimentos satisfatórios para gerir adequadamente os aspetos da cibersegurança abrangidos pelo presente regulamento.

5.3.1. A entidade homologadora e os seus serviços técnicos devem assegurar, para além dos critérios enunciados no anexo 2 do Acordo de 1958:

a) Que dispõem de pessoal competente em cibersegurança e conhecimentos específicos em matéria de avaliação dos riscos no setor automóvel ([1]);

b) Que aplicaram os procedimentos para a avaliação uniforme conformes com o presente regulamento.

5.3.2. Cada Parte Contratante que aplique o presente regulamento deve notificar e informar, por intermédio da sua entidade homologadora, outras entidades de homologação das Partes Contratantes que apliquem o presente regulamento da ONU sobre o método e os critérios que servem de base à entidade notificadora para avaliar a adequação das medidas tomadas em conformidade com o presente regulamento e, em especial, com os pontos 5.1, 7.2 e 7.3.

Estas informações devem ser comunicadas a) apenas antes da concessão da primeira homologação em conformidade com o presente regulamento e b) cada vez que o método ou os critérios de avaliação forem atualizados.

Estas informações destinam-se a ser partilhadas para efeitos de compilação e análise das melhores práticas e a fim de garantir a aplicação convergente das disposições por todas as entidades homologadoras que aplicam o presente regulamento.

5.3.3. As informações referidas no ponto 5.3.2 devem ser carregadas em língua inglesa na base de dados disponível num sítio da Internet seguro «DETA» ([2]), criada pela Comissão Económica das Nações Unidas para a Europa, em tempo útil e o mais tardar 14 dias antes da concessão da primeira homologação segundo os métodos e critérios de avaliação pertinentes. As informações devem ser suficientes para permitir compreender os níveis de desempenho mínimos que a entidade homologadora adotou para cada um dos requisitos específicos referidos no ponto 5.3.2, bem como os processos e medidas que aplica para verificar se esses níveis mínimos de desempenho são cumpridos ([3]).

5.3.4. As entidades homologadoras que recebem as informações a que se refere o ponto 5.3.2 podem apresentar observações à entidade homologadora notificadora, carregando-as na DETA no prazo de 14 dias a contar do dia da notificação.

5.3.5. Se não for possível à entidade homologadora que concede uma homologação ter em conta as observações recebidas em conformidade com o ponto 5.3.4, as entidades homologadoras que tenham enviado observações e a entidade homologadora que concede uma homologação devem solicitar esclarecimentos adicionais, em conformidade com o anexo 6 do Acordo de 1958. O grupo de trabalho subsidiário competente ([4]) do Fórum Mundial para a Harmonização das Regulamentações aplicáveis a Veículos (WP.29) do presente regulamento deve chegar a acordo sobre uma interpretação comum dos métodos e critérios de avaliação ([5]). Essa interpretação comum deve ser aplicada e todas as entidades homologadoras devem conceder homologações em conformidade com o presente regulamento.

([1]) Ver, por exemplo, as normas ISO 26262-2018, ISO/PAS 21448 e ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) As orientações relativas às informações pormenorizadas (por exemplo, método, critérios, nível de desempenho) a carregar e o formato a utilizar devem ser fornecidos no documento de interpretação que o Grupo de trabalho informal da cibersegurança e das questões de segurança das transmissões sem fios está a preparar para a sétima sessão do GRVA.
([4]) Grupo de Trabalho dos veículos automatizados/autónomos e conectados (GRVA).
([5]) Esta interpretação deve refletir-se no documento de interpretação referido na nota de rodapé do ponto 5.3.3.

5.3.6. Cada entidade homologadora que conceda uma homologação em conformidade com o presente regulamento deve notificar as outras entidades homologadoras. A homologação e a documentação complementar devem ser carregadas na DETA, em inglês, pela entidade homologadora no prazo de 14 dias a contar da data de concessão da homologação ([6]).

5.3.7. As Partes Contratantes podem estudar as homologações concedidas com base nas informações carregadas em conformidade com o ponto 5.3.6. Quaisquer divergências de pontos de vista entre as Partes Contratantes devem ser resolvidas em conformidade com o artigo 10.º e o anexo 6 do Acordo de 1958. As Partes Contratantes devem informar igualmente o grupo de trabalho subsidiário competente do Fórum Mundial para a Harmonização das Regulamentações aplicáveis a Veículos (WP.29) sobre as interpretações divergentes na aceção do anexo 6 do Acordo de 1958. O grupo de trabalho competente deve contribuir para a resolução das divergências de pontos de vista e pode consultar o WP.29 sobre essa questão, se necessário.

5.4. Para efeitos do ponto 7.2 do presente regulamento, o fabricante deve assegurar a aplicação dos aspetos de cibersegurança abrangidos pelo presente regulamento.

6. Certificado de conformidade do sistema de gestão da cibersegurança

6.1. As Partes Contratantes devem nomear uma entidade homologadora para efetuar a avaliação do fabricante e emitir um certificado de conformidade do CSMS.

6.2. O pedido de certificado de conformidade do sistema de gestão da cibersegurança deve ser apresentado pelo fabricante do veículo ou pelo seu representante devidamente acreditado.

6.3. O pedido deve ser acompanhado pelos documentos a seguir mencionados, em triplicado, e pelo seguinte:

6.3.1. Documentos que descrevem o sistema de gestão da cibersegurança;

6.3.2. Uma declaração assinada conforme ao modelo definido no apêndice 1 do anexo 1.

6.4. No contexto da avaliação, o fabricante deve declarar, utilizando o modelo definido no apêndice 1 do anexo 1, e demonstrar, a contento da entidade homologadora ou do seu serviço técnico, que dispõe dos processos necessários para cumprir todos os requisitos da cibersegurança nos termos do presente regulamento.

6.5. Quando esta avaliação tiver sido concluída satisfatoriamente e depois de receber uma declaração assinada do fabricante de acordo com o modelo definido no apêndice 1 do anexo 1, será concedido ao fabricante um certificado de conformidade do CSMS tal como descrito no anexo 4 do presente regulamento (a seguir designado por «Certificado de conformidade do CSMS»).

6.6. A entidade homologadora ou o seu serviço técnico devem utilizar o modelo constante do anexo 4 do presente regulamento para o certificado de conformidade do CSMS.

6.7. O certificado de conformidade do CSMS deve permanecer válido por um período máximo de três anos a contar da data de entrega do certificado, exceto se for revogado.

6.8. A entidade homologadora que emitiu o certificado de conformidade do CSMS pode, em qualquer altura, verificar se os requisitos para o mesmo continuam a ser cumpridos. A entidade homologadora deve revogar o certificado de conformidade do CSMS se os requisitos estabelecidos no presente regulamento deixarem de ser cumpridos.

([6]) Mais informações sobre os requisitos mínimos para o dossiê de documentação serão desenvolvidas pelo GRVA durante a sua sétima sessão.

6.9. O fabricante deve informar a entidade homologadora ou o seu serviço técnico sobre qualquer alteração que afete a relevância do certificado de conformidade do CSMS. Após ter consultado o fabricante, a entidade homologadora ou o seu serviço técnico devem decidir se são necessárias novas verificações.

6.10. O fabricante deve pedir um novo certificado de conformidade do CSMS, ou a sua prorrogação em devido tempo, permitindo à entidade homologadora concluir a sua avaliação antes do termo do período de validade do certificado de conformidade do CSMS. Sem prejuízo de uma avaliação favorável, a entidade homologadora deve emitir um novo certificado de conformidade do CSMS ou prorrogar a sua validade por mais um período de três anos. A entidade homologadora deve verificar se o CSMS continua a cumprir os requisitos do presente regulamento. A entidade homologadora deve emitir um novo certificado nos casos em que tenham sido comunicadas alterações à entidade homologadora ou ao seu serviço técnico e em que as alterações tenham sido reavaliadas favoravelmente.

6.11. A caducidade ou a retirada do certificado de conformidade do CSMS do fabricante deve ser considerada, no que diz respeito aos modelos de veículos para os quais o CSMS em causa era pertinente, como modificação da homologação, tal como referido no ponto 8, o que pode implicar a revogação da homologação, se já não estiverem preenchidas as condições para a concessão da homologação.

7. Especificações

7.1. Especificações gerais

7.1.1. Os requisitos do presente regulamento não restringem as disposições ou os requisitos de outros regulamentos da ONU.

7.2. Requisitos relativos ao sistema de gestão da cibersegurança

7.2.1. Com vista à avaliação, a entidade homologadora ou o seu serviço técnico devem verificar se o fabricante do veículo dispõe de um sistema de gestão da cibersegurança e deve verificar a sua conformidade com o presente regulamento.

7.2.2. O sistema de gestão da cibersegurança deve cobrir os seguintes aspetos:

7.2.2.1. O fabricante do veículo deve demonstrar à entidade homologadora ou ao serviço técnico que o seu sistema de gestão da cibersegurança se aplica às seguintes fases:

a) Fase de desenvolvimento;

b) Fase de produção;

c) Fase de pós-produção.

7.2.2.2. O fabricante do veículo deve demonstrar que os processos utilizados no seu sistema de gestão da cibersegurança asseguram a devida consideração da segurança, incluindo os riscos e medidas de mitigação enumerados no anexo 5. Estes processos incluem:

a) Os processos utilizados na organização do fabricante para gerir a cibersegurança;

b) Os processos utilizados para identificação dos riscos a que estão expostos os modelos de veículo. No âmbito destes processos, devem ser consideradas as ameaças constantes do anexo 5, parte A, e outras ameaças pertinentes;

c) Os processos utilizados para apreciação, categorização e tratamento dos riscos identificados;

d) Os processos em vigor para verificar se os riscos identificados são geridos de forma adequada;

e) Os processos utilizados para controlar a cibersegurança de um modelo de veículo;

f) Os processos utilizados para garantir que a avaliação dos riscos se mantém atualizada;

g) Os processos utilizados para monitorizar, detetar e responder a ciberataques, ciberameaças e vulnerabilidades nos modelos de veículos e os processos utilizados para avaliar se as medidas de cibersegurança aplicadas continuam a ser eficazes à luz das novas ciberameaças e vulnerabilidades que foram identificadas;

h) Os processos utilizados para recolher dados pertinentes para apoiar a análise de ciberataques tentados ou consumados.

7.2.2.3. O fabricante do veículo deve demonstrar que os processos utilizados no seu sistema de gestão da cibersegurança garantem que, com base na categorização referida no ponto 7.2.2.2, alíneas c) e g), as ciberameaças e as vulnerabilidades que exijam uma resposta do fabricante do veículo devem ser mitigadas num prazo razoável.

7.2.2.4. O fabricante do veículo deve demonstrar que os processos utilizados no seu sistema de gestão da cibersegurança garantem que a monitorização referida no ponto 7.2.2.2, alínea g), é permanente. Tal deve:

a) Incluir na monitorização veículos após o primeiro registo;

b) Incluir a capacidade de analisar e detetar ciberameaças, vulnerabilidades e ciberataques a partir dos dados do veículo e dos registos do veículo. Esta capacidade deve cumprir o disposto no ponto 1.3 e os direitos de privacidade dos proprietários ou condutores dos veículos, nomeadamente no que diz respeito ao consentimento.

7.2.2.5. O fabricante do veículo deve ser obrigado a demonstrar de que forma o seu sistema de gestão da cibersegurança irá gerir as dependências que possam existir com os fornecedores contratados, os prestadores de serviços ou as suborganizações do fabricante, no que respeita aos requisitos do ponto 7.2.2.2.

7.3. Requisitos relativos aos modelos de veículos

7.3.1. O fabricante deve dispor de um certificado de conformidade válido para o sistema de gestão da cibersegurança correspondente ao modelo de veículo a homologar. Todavia, para as homologações de veículos das categorias M, N e O emitidas pela primeira vez antes de 1 de julho de 2024 e para as homologações de veículos da categoria L emitidas pela primeira vez antes de 1 de julho de 2029 e respetivas extensões, se o fabricante do veículo puder demonstrar que o modelo de veículo não pôde ser desenvolvido em conformidade com o sistema de gestão da cibersegurança, então o fabricante do veículo deve demonstrar que a cibersegurança foi devidamente tida em conta durante a fase de desenvolvimento do modelo de veículo em questão.

7.3.2. O fabricante do veículo deve identificar e gerir, para o modelo de veículo a homologar, os riscos relacionados com os fornecedores.

7.3.3. O fabricante do veículo deve identificar os elementos críticos do modelo de veículo, efetuar uma avaliação exaustiva dos riscos para esse modelo de veículo e tratar ou gerir adequadamente os riscos identificados. A avaliação dos riscos deve ter em conta os elementos individuais do modelo de veículo e as suas interações. A avaliação dos riscos deve ainda ter em conta as interações com quaisquer sistemas externos. Ao avaliar os riscos, o fabricante do veículo deve ter em conta os riscos relacionados com todas as ameaças referidas no anexo 5, parte A, assim como qualquer outro risco pertinente.

7.3.4. O fabricante do veículo deve proteger o modelo de veículo contra os riscos identificados na sua apreciação dos riscos devendo, para esse fim, ser aplicadas medidas de mitigação proporcionadas. As medidas de mitigação aplicadas incluem todas as medidas referidas no anexo 5, partes B e C, que são pertinentes para os riscos identificados. Contudo, se uma medida de mitigação referida no anexo 5, partes B ou C, não for pertinente ou não for suficiente para o risco identificado, o fabricante do veículo deve assegurar a aplicação de outra medida de mitigação adequada.

Em especial, no que se refere às homologações de veículos das categorias M, N e O emitidas pela primeira vez antes de 1 de julho de 2024 e às homologações de veículos da categoria L emitidas pela primeira vez antes de 1 de julho de 2029 e respetivas extensões, o fabricante do veículo deve assegurar a aplicação de outra medida de mitigação adequada se não for tecnicamente viável aplicar uma das medidas de mitigação referidas no anexo 5, parte B ou C. O fabricante deve apresentar à entidade homologadora a respetiva avaliação da viabilidade técnica.

7.3.5. O fabricante do veículo deve pôr em prática medidas adequadas e proporcionadas para garantir a segurança de ambientes específicos no modelo de veículo (se fornecidos) para o armazenamento e a execução de *software*, serviços, aplicações ou dados pós-venda.

7.3.6. O fabricante do veículo deve realizar ensaios adequados e suficientes, antes da homologação, para verificar a eficácia das medidas de segurança aplicadas.

7.3.7. O fabricante do veículo deve aplicar medidas para o modelo de veículo a fim de:

a) Detetar e prevenir ciberataques contra veículos desse modelo;

b) Reforçar a sua capacidade de monitorização para deteção de ameaças, vulnerabilidades e ciberataques pertinentes para o modelo de veículo;

c) Dispor da capacidade de investigação forense para permitir a análise de ciberataques tentados ou consumados.

7.3.8. Os módulos criptográficos utilizados para efeitos do presente regulamento devem estar em conformidade com as normas consensuais. Se os módulos criptográficos utilizados não estiverem em conformidade com as normas consensuais, o fabricante do veículo deve justificar a sua utilização.

7.4. Disposições em matéria de comunicação de informações

7.4.1. O fabricante do veículo deve comunicar, pelo menos uma vez por ano, ou com maior frequência se tal for relevante, à entidade homologadora ou ao serviço técnico o resultado das suas atividades de monitorização, tal como definido no ponto 7.2.2.2, alínea g), incluindo nomeadamente as informações relativas a novos ciberataques. O fabricante do veículo deve também comunicar e confirmar à entidade homologadora ou ao serviço técnico que as medidas de mitigação em matéria de cibersegurança aplicadas para os seus modelos de veículos continuam a ser eficazes e comunicar eventuais medidas adicionais tomadas.

7.4.2. A entidade homologadora ou o serviço técnico deve verificar as informações fornecidas e, se necessário, exigir que o fabricante do veículo corrija qualquer ineficácia detetada.

Se as informações comunicadas ou a resposta não forem suficientes, a entidade homologadora pode decidir revogar o CSMS em conformidade com o ponto 6.8.

8. Modificação do modelo de veículo e extensão da homologação

8.1. Todas as modificações do modelo de veículo que afetem o seu desempenho técnico no que respeita à cibersegurança e/ou à documentação exigida no presente regulamento devem ser notificadas à entidade homologadora que homologou o modelo de veículo. A entidade homologadora pode então:

8.1.1. Considerar que as modificações feitas continuam a cumprir os requisitos e a documentação da homologação existente; ou

8.1.2. Proceder à necessária avaliação complementar nos termos do ponto 5 e exigir, se for caso disso, um novo relatório de ensaio do serviço técnico responsável pela realização dos ensaios.

8.1.3. A confirmação, extensão ou recusa da homologação, com especificação das alterações introduzidas, deve ser comunicada através de um formulário de comunicação conforme ao modelo apresentado no anexo 2 do presente regulamento. A entidade homologadora responsável pela extensão da homologação atribui um número de série a essa extensão e informa do facto as restantes partes no Acordo de 1958 que apliquem o presente regulamento, por meio de um formulário de comunicação conforme ao modelo apresentado no anexo 2 do presente regulamento.

9. Conformidade da produção

9.1. Os procedimentos relativos à conformidade da produção devem cumprir o disposto no Acordo de 1958, anexo 1 (E/ECE/TRANS/505/Rev.3), bem como as seguintes disposições:

9.1.1. O titular da homologação deve assegurar que os resultados dos ensaios relativos à conformidade da produção são registados e que os documentos em anexo se mantêm disponíveis durante um período a determinar em concertação com a entidade homologadora ou o seu serviço técnico. O referido período não deve exceder 10 anos, a contar da data em que a produção cessou de forma definitiva;

9.1.2. A entidade que tiver concedido a homologação pode verificar, em qualquer momento, os métodos de controlo da conformidade aplicados em cada unidade de produção. A periodicidade normal dessas verificações é a cada três anos.

10. Sanções por não conformidade da produção

10.1. A homologação concedida a um modelo de veículo nos termos do presente regulamento pode ser revogada se os requisitos enunciados no presente regulamento não forem cumpridos ou se os veículos-amostra não cumprirem os requisitos do presente regulamento.

10.2. Se uma entidade homologadora revogar uma homologação previamente concedida, deve notificar imediatamente desse facto as partes contratantes que apliquem o presente regulamento, utilizando um formulário de comunicação conforme ao modelo constante do anexo 2 do presente regulamento.

11. Cessação definitiva da produção

11.1. Se o titular da homologação deixar definitivamente de fabricar um modelo de veículo homologado nos termos do presente regulamento, deve informar desse facto a entidade homologadora. Após receber a comunicação, essa autoridade deve do facto informar as outras partes contratantes no acordo que aplicam o presente regulamento por meio de uma cópia do certificado de homologação que ostente no final, em letras grandes, a anotação, assinada e datada, «CESSAÇÃO DA PRODUÇÃO».

12. Designações e endereços dos serviços técnicos responsáveis pela realização dos ensaios de homologação e das entidades homologadoras

12.1. As partes contratantes no Acordo que apliquem o presente regulamento comunicam ao Secretariado das Nações Unidas as designações e os endereços dos serviços técnicos responsáveis pela realização dos ensaios de homologação e das entidades homologadoras que concedem as homologações e aos quais devem ser enviados os certificados de concessão, extensão, recusa ou revogação da homologação emitidos noutros países.

ANEXO 1

Ficha de informações

Se for caso disso, as informações a seguir indicadas devem ser fornecidas em triplicado e incluir um índice. Caso existam, os desenhos devem ser fornecidos à escala adequada e com pormenor suficiente, em formato A4 ou dobrados nesse formato. Eventuais fotografias, com grau de pormenor suficiente.

1. Marca (designação comercial do fabricante):.....

2. Tipo e designação(ões) comercial(is) geral(is): .....

3. Meios de identificação do modelo/tipo, se marcados no veículo:.....

4. Localização dessa marcação:.....

5. Categoria(s) do veículo:.....

6. Nome e endereço do fabricante ou do seu representante: .....

7. Nome(s) e endereço(s) da(s) instalação(ões) de montagem: .....

8. Fotografia(s) e/ou desenho(s) de um veículo representativo:.....

9. Cibersegurança

9.1. Características gerais de construção do modelo de veículo, incluindo:

a) Os sistemas do veículo pertinentes para a cibersegurança do modelo de veículo;

b) Os componentes desses sistemas que são pertinentes para a cibersegurança;

c) As interações desses sistemas com outros sistemas no interior do modelo de veículo e nas interfaces externas.

9.2. Representação esquemática do modelo de veículo

9.3. Número do certificado de conformidade do CSMS: .....

9.4. Documentos relativos ao modelo de veículo a homologar que descrevem os resultados da avaliação dos riscos e os riscos identificados:.....

9.5. Documentos relativos ao modelo de veículo a homologar que descrevem as medidas de mitigação que foram aplicadas nos sistemas listados, ou no modelo de veículo, e a forma como fazer face aos riscos declarados:.....

9.6. Documentos relativos ao modelo de veículo a homologar que descrevem a proteção de ambientes específicos para *software*, serviços, aplicações ou dados pós-venda:.....

9.7. Documentos relativos ao modelo de veículo a homologar que descrevem os ensaios efetuados para verificar a cibersegurança do modelo de veículo e dos seus sistemas e os resultados desses ensaios: .....

9.8. Descrição da análise da cadeia de abastecimento no que diz respeito à cibersegurança: .....

Anexo 1 — Apêndice 1

Modelo de declaração de conformidade do CSMS a preencher pelo fabricante

Declaração do fabricante relativa à conformidade com os requisitos para o sistema de gestão da cibersegurança

Nome do fabricante: .....

Endereço do fabricante: .....

..... (*Nome do fabricante*)

atesta que os processos necessários para cumprir os requisitos relativos ao sistema de gestão da cibersegurança enunciados no ponto 7.2 do Regulamento n.º 155 da ONU estão instalados e serão mantidos.

Feito em: .....(*local*)

Data: .....

Nome do signatário: .....

Função do signatário: .....

(Carimbo e assinatura do representante do fabricante)

ANEXO 2

Comunicação

[Formato máximo: A4 (210 × 297 mm)]



emitida por: Designação da entidade administrativa:
.....
.....
.....

Referente a: (2) Concessão da homologação
Extensão da homologação
Revogação da homologação com efeitos a partir de dd/mm/aaaa
Recusa da homologação
Cessação definitiva da produção

de um modelo de veículo nos termos do Regulamento n.º 155 da ONU

N.º de homologação:.....

N.º de extensão:.....

Razão da extensão: .....

1. Marca (designação comercial do fabricante):.....

2. Modelo/tipo e designação(ões) comercial(ais) geral(ais): .....

3. Meios de identificação do modelo/tipo, se marcados no veículo:.....

3.1. Localização dessa marcação:.....

4. Categoria(s) do veículo:.....

5. Nome e endereço do fabricante ou do seu representante: .....

6. Nome(s) e endereço(s) da(s) instalação(ões) de produção:.....

7. Número do certificado de conformidade do sistema de gestão da cibersegurança: .....

8. Serviço técnico responsável pela realização dos ensaios: .....

9. Data do relatório de ensaio: .....

10. Número do relatório de ensaio:.....

11. Observações (se for caso disso): .....

12. Local: .....

(1) Número distintivo do país que procedeu à concessão/extensão/recusa/revogação da homologação (ver disposições de homologação no texto do regulamento).
(2) Riscar o que não interessa.

13. Data:……

14. Assinatura:……

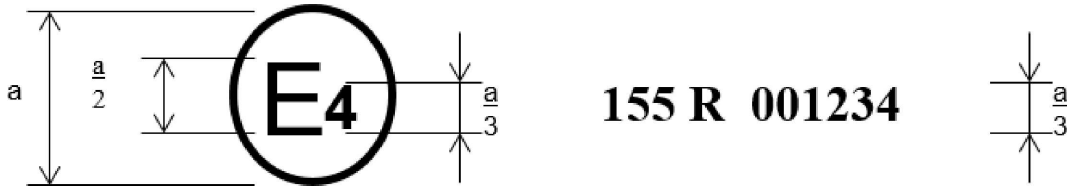
15. Encontra-se em anexo o índice do dossiê de homologação, que está arquivado junto da entidade homologadora e pode ser obtido a pedido.

ANEXO 3

Exemplo de marca de homologação

MODELO A

(Ver ponto 4.2 do presente regulamento)



a = 8 mm mín.

A marca de homologação acima indicada, afixada num veículo, indica que o modelo de veículo em causa foi homologado nos Países Baixos (E4), nos termos do Regulamento n.º 155, com o número de homologação 001234. Os dois primeiros algarismos deste número indicam que a homologação foi concedida em conformidade com os requisitos do presente regulamento na sua forma original (00).

ANEXO 4

MODELO DE CERTIFICADO DE CONFORMIDADE DO CSMS

Certificado de conformidade do sistema de gestão da cibersegurança

com o Regulamento n.º 155 da ONU

Número do certificado [*número de referência*]

[… *entidade homologadora*]

Certifica que

Fabricante: ……

Endereço do fabricante: ……

está em conformidade com o disposto no ponto 7.2 do Regulamento n.º 155.

Foram realizadas verificações em: ……

pelo/a (nome e endereço da entidade homologadora ou do serviço técnico): ……

Número do relatório: ……

O presente certificado é válido até […… *Data*]

Feito em […… *Local*]

Em […… *Data*]

[…… *Assinatura*]

Anexos: descrição do sistema de gestão da cibersegurança elaborada pelo fabricante.

ANEXO 5

Lista de ameaças e respetivas medidas de mitigação

1. O presente anexo é composto por três partes. A parte A descreve a linha de base de ameaças, vulnerabilidades e métodos de ataque. A parte B descreve as medidas de mitigação das ameaças que visam modelos de veículos. A parte C descreve as medidas de mitigação das ameaças que visam áreas fora dos veículos, por exemplo, sistemas informáticos de apoio de retaguarda.

2. A parte A, a parte B e a parte C devem ser consideradas para efeitos de avaliação dos riscos e de medidas de mitigação a aplicar pelos fabricantes de veículos.

3. A vulnerabilidade de alto nível e os exemplos correspondentes foram indexados na parte A. A mesma indexação foi referenciada nos quadros das partes B e C para estabelecer uma ligação entre cada ataque ou vulnerabilidade e uma lista de medidas de mitigação correspondentes.

4. A análise das ameaças deve também incluir um exame de eventuais consequências de um ataque. Este exame pode contribuir para determinar o grau de risco e identificar riscos adicionais. Eventuais consequências de um ataque podem:

   a) Comprometer a utilização do veículo em condições de segurança;

   b) Interromper funções do veículo;

   c) Modificar o *software* e alterar o desempenho;

   d) Alterar o *software* sem efeitos no funcionamento;

   e) Comprometer a integridade dos dados;

   f) Comprometer a confidencialidade dos dados;

   g) Impedir o acesso aos dados;

   h) Ser outras ligadas à criminalidade.

PARTE A

Vulnerabilidades ou métodos de ataque relacionados com as ameaças

As descrições de alto nível das ameaças e das vulnerabilidades ou dos métodos de ataque correspondentes constam do quadro A1.

Quadro A1

Lista de vulnerabilidades ou de métodos de ataque relacionados com as ameaças

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
4.3.1. Ameaças para os servidores de apoio de retaguarda relacionadas com veículos em circulação	1	Servidores de apoio de retaguarda utilizados para atacar um veículo ou extrair dados	1.1	Utilização abusiva de privilégios pelo pessoal (ataque interno)
			1.2	Acesso não autorizado ao servidor através da Internet (ativado, por exemplo, por função-alçapão, vulnerabilidades do sistema de *software* não corrigidas, ataques SQL ou outros meios)
			1.3	Acesso físico não autorizado ao servidor (por meio, por exemplo, de memória USB ou outro suporte de ligação ao servidor)
	2	Perturbação dos serviços de servidor de apoio de retaguarda que afetam o funcionamento de um veículo	2.1	Ataque ao servidor de apoio de retaguarda que bloqueia o seu funcionamento, por exemplo, impede-o de interagir com os veículos e de fornecer serviços dos quais dependem

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
	3	Dados relativos a veículos, guardados em servidores de apoio de retaguarda, perdidos ou comprometidos («violação de dados»)	3.1	Utilização abusiva de privilégios pelo pessoal (ataque interno)
			3.2	Perda de informações na «nuvem». Dados sensíveis podem ser perdidos devido a ataques ou incidentes quando os dados são armazenados por terceiros prestadores de serviços de computação em «nuvem»
			3.3	Acesso não autorizado ao servidor através da Internet (ativado, por exemplo, por função-alçapão, vulnerabilidades do sistema de *software* não corrigidas, ataques SQL ou outros meios)
			3.4	Acesso físico não autorizado ao servidor (por meio, por exemplo, de memória USB ou outro suporte de ligação ao servidor)
			3.5	Violação de informações através da partilha acidental de dados (por exemplo, erros administrativos)
4.3.2 Ameaças para os veículos no que respeita aos seus canais de comunicação	4	Simulação de mensagens ou de dados recebidos pelo veículo	4.1	Simulação de mensagens por disfarce de identidade pessoal (por exemplo, mensagens de perceção cooperativa ou coordenação de manobras entre o veículo e o ambiente — V2X, mensagens GNSS, etc.)
			4.2	Ataque Sybil (visando simular outros veículos para fazer crer que há muitos na estrada)
	5	Canais de comunicação utilizados para efetuar manipulações, supressões ou outras alterações não autorizadas do código ou dos dados do veículo	5.1	Os canais de comunicação permitem a injeção de códigos, por exemplo, um código binário de software manipulado pode ser injetado no fluxo de comunicação
			5.2	Os canais de comunicação permitem manipular os dados ou o código do veículo
			5.3	Os canais de comunicação permitem substituir os dados ou o código do veículo
			5.4	Os canais de comunicação permitem suprimir os dados ou o código do veículo
			5.5	Os canais de comunicação permitem a introdução de dados ou de código no veículo (escrever o código ou dados)
	6	Os canais de comunicação permitem que mensagens não fiáveis sejam aceites ou são vulneráveis a sequestro de sessão ou a ataques de replicação	6.1	Aceitação de informações provenientes de uma fonte não fiável
			6.2	Ataque de homem no meio (comunicação intercetada)/sequestro de sessão
			6.3	Ataque de replicação, por exemplo um ataque contra um portal de comunicação permite ao atacante instalar uma versão anterior do *software* de uma UCE ou de um microprograma (*firmware*) do portal
	7	As informações podem ser facilmente divulgadas. Por exemplo, através de interceção de comunicações ou permitindo acesso não autorizado a ficheiros ou pastas sensíveis	7.1	Interceção de informações/ radiações perturbadoras/ monitorização de comunicações
			7.2	Obtenção de acesso não autorizado a ficheiros ou dados

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
	8	Ataques de negação de serviço através de canais de comunicação para perturbar as funções do veículo	8.1	Envio de um grande número de dados parasitas ao sistema de informação do veículo, de modo a que este seja incapaz de prestar os serviços normalmente
			8.2	Ataque por buraco negro, visando perturbar a comunicação entre os veículos, o atacante é capaz de bloquear mensagens entre os veículos
	9	Um utilizador não privilegiado pode obter um acesso privilegiado aos sistemas do veículo	9.1	Um utilizador não privilegiado pode obter um acesso privilegiado, por exemplo, à raiz do sistema
	10	Vírus incorporados nos meios de comunicação podem infetar os sistemas do veículo	10.1	Um vírus incorporado nos meios de comunicação infeta os sistemas do veículo
	11	As mensagens recebidas pelo veículo (por exemplo, mensagens X2V ou de diagnóstico), ou transmitidas no seu interior, contêm conteúdo malicioso	11.1	Mensagens internas (por exemplo, CAN) maliciosas
			11.2	Mensagens V2X maliciosas, por exemplo, mensagens de infraestrutura para o veículo ou de veículo a veículo (por exemplo, CAM, DENM)
			11.3	Mensagens de diagnóstico maliciosas
			11.4	Mensagens proprietárias maliciosas (por exemplo, as normalmente enviadas a partir de OEM ou de fornecedores de componentes/sistemas/funções)
4.3.3. Ameaças para os veículos ligadas aos seus procedimentos de atualização	12	Utilização abusiva ou comprometimento de procedimentos de atualização	12.1	Comprometimento dos procedimentos de atualização sem fios do *software*, incluindo o fabrico do programa ou do microprograma (*firmware*) de atualização do sistema
			12.2	Comprometimento dos procedimentos de atualização locais/físicos do *software*, incluindo o fabrico do programa ou do microprograma (*firmware*) de atualização do sistema
			12.3	O *software* é manipulado antes do processo de atualização (e, por isso, está corrompido), embora o processo de atualização esteja intacto
			12.4	Comprometimento das chaves criptográficas do fornecedor de *software* visando permitir uma atualização não válida
	13	Possibilidade de impedir atualizações legítimas	13.1	Ataque de negação de serviço contra o servidor ou a rede de atualização para impedir a disponibilização de atualizações de *software* crítico e/ou desbloquear funcionalidades específicas do cliente
4.3.4. Ameaças para veículos ligadas a ações humanas não intencionais que facilitem um ciberataque	15	Atores legítimos podem tomar medidas que facilitem involuntariamente um ciberataque	15.1	Vítima inocente (por exemplo, proprietário, operador ou engenheiro de manutenção) enganado e levado a carregar um programa malicioso (*malware*) de forma não intencional ou a permitir um ataque
			15.2	Os procedimentos de segurança definidos não são seguidos

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
4.3.5. Ameaças para os veículos ligadas à sua conectividade e às suas conexões externas	16	A manipulação da conectividade das funções do veículo permite um ciberataque, podendo incluir telemática; sistemas que permitem operações à distância e sistemas que utilizam comunicações sem fios de curto alcance	16.1	Manipulação de funções concebidas para comandar sistemas à distância, como uma chave remota, um dispositivo de imobilização e um posto de carregamento
			16.2	Manipulação da telemática do veículo (por exemplo, manipulação da medição de temperatura de mercadorias sensíveis, desbloqueio à distância das portas de carga)
			16.3	Interferência com sistemas ou sensores sem fios de curto alcance
	17	Utilização de *software* de terceiros, por exemplo, aplicações de entretenimento, para atacar os sistemas do veículo	17.1	Utilização de aplicações corrompidas, ou cuja segurança de *software* é deficiente, para atacar sistemas do veículo
	18	Utilização de dispositivos conectados a interfaces externas, por exemplo, portas USB ou porta OBD, para atacar os sistemas do veículo	18.1	Interfaces externas, tais como portas USB ou outras, utilizadas como ponto de ataque, por exemplo através de injeção de código
			18.2	Suporte infetado com um vírus conectado a um sistema do veículo
			18.3	Acesso diagnóstico (por exemplo, dispositivos de conexão à porta OBD) utilizado para facilitar um ataque, por exemplo, manipular (direta ou indiretamente) parâmetros do veículo
4.3.6. Ameaças para os dados ou o código do veículo	19	Extração dos dados ou do código do veículo	19.1	Extração de *software* proprietário ou com direitos de autor dos sistemas do veículo (pirataria de produtos)
			19.2	Acesso não autorizado às informações privadas do proprietário, tais como a sua identidade, contas de pagamento, livro de endereços, informações sobre a sua localização, identificação eletrónica do veículo, etc.
			19.3	Extração de chaves criptográficas
	20	Manipulação dos dados ou do código do veículo	20.1	Alterações ilícitas/não autorizadas da identificação eletrónica do veículo
			20.2	Fraude de identidade. Por exemplo, se um utilizador pretender apresentar outra identidade ao comunicar com os sistemas de portagem, o sistema dorsal do fabricante
			20.3	Medida para contornar os sistemas de monitorização (por exemplo, pirataria informática/manipulação/bloqueio de mensagens, tal como dados de ODR Tracker ou o número de execuções)
			20.4	Manipulação de dados que falsifique os dados de condução do veículo (por exemplo, quilometragem, velocidade de condução, itinerários, etc.)
			20.5	Alterações não autorizadas dos dados de diagnóstico do sistema
	21	Supressão dos dados ou do código	21.1	Supressão/manipulação não autorizada dos registos de eventos do sistema
	22	Introdução de *software* malicioso	22.2	Introduzir *software* malicioso ou atividade de *software* malicioso

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
	23	Introdução de novo *software* ou reescrita de *software* existente	23.1	Fabrico de *software* do sistema de comando ou de informação do veículo
	24	Perturbação dos sistemas ou das operações	24.1	Negação de serviço, que pode, por exemplo, ser desencadeada na rede interna, inundando um barramento CAN ou provocando avarias numa UCE através de uma elevada taxa de envio de mensagens
	25	Manipulação dos parâmetros do veículo	25.1	Acesso não autorizado visando falsificar os parâmetros de configuração das funções críticas do veículo, tais como os dados de travagem, o limiar de projeção do saco insuflável (*airbag*), etc.
			25.2	Acesso não autorizado visando falsificar os parâmetros de carga, tais como a tensão de carga, a potência de carga, a temperatura da bateria, etc.
4.3.7. Vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas	26	As tecnologias criptográficas podem estar comprometidas ou não ser suficientemente aplicadas	26.1	A combinação de chaves criptográficas curtas e um longo período de validade permite ao atacante quebrar a cifragem
			26.2	Recurso insuficiente aos algoritmos criptográficos para proteger os sistemas vulneráveis
			26.3	Utilização de algoritmos criptográficos obsoletos, ou que o serão em breve
	27	Peças ou fornecimentos podem ser comprometidos para permitir o ataque aos veículos	27.1	*Hardware* ou *software* concebido para permitir um ataque ou que não cumpre os critérios de conceção para impedir um ataque
	28	A conceção do *software* ou *hardware* permite vulnerabilidades	28.1	Erros de *software*. A presença de erros de *software* pode constituir uma base para vulnerabilidades suscetíveis de ser exploradas, particularmente se o software não tiver sido testado para verificar a ausência de códigos errados ou de erros conhecidos e para reduzir o risco da presença de outros desconhecidos
			28.2	A utilização de restos da fase de desenvolvimento (por exemplo, portas de correção, portas JTAG, microprocessadores, certificados de desenvolvimento, senhas de desenvolvimento, etc.) pode permitir o acesso às unidades de controlo eletrónico (UCE) ou permitir a atacantes obter privilégios mais elevados
	29	A conceção das redes introduz vulnerabilidades	29.1	Portas de Internet supérfluas deixadas abertas, que dão acesso aos sistemas de rede
			29.2	Contornar a separação das redes para obter controlo. Um exemplo específico é a utilização de portais de acesso ou pontos de acesso não protegidos (tais como as portais de acesso de camião-reboque) para contornar as proteções e obter acesso a outros segmentos da rede com vista a cometer atos maliciosos, como o envio de mensagens arbitrárias do barramento CAN
	31	A transferência não intencional de dados pode ocorrer	31.1	Violação de informações. Os dados pessoais podem ser divulgados quando o automóvel muda de utilizador (por exemplo, em caso de venda ou de utilização como veículo de aluguer por novos clientes)

Descrições de alto nível e de subnível da vulnerabilidade/ameaça			Exemplo de vulnerabilidade ou de método de ataque	
	32	A manipulação física dos sistemas pode permitir um ataque	32.1	Manipulação do equipamento eletrónico, por exemplo equipamento eletrónico não autorizado adicionado a um veículo para permitir um ataque por interceção («homem no meio») Substituição de *hardware* eletrónico autorizado (por exemplo, sensores) por *hardware* eletrónico não autorizado Manipulação das informações recolhidas por um sensor (por exemplo, utilização de um íman para manipular o sensor de efeitos de Hall ligado à caixa de velocidades)

PARTE B

Medidas de mitigação das ameaças que visam os veículos

1. Medidas de mitigação para «canais de comunicação dos veículos»

As medidas de mitigação das ameaças relacionadas com os «canais de comunicação dos veículos» constam do quadro B1.

Quadro B1

Medidas de mitigação das ameaças relacionadas com os «canais de comunicação dos veículos»

Referência do quadro A1	Ameaças aos «canais de comunicação dos veículos»	Ref	Medidas de mitigação
4.1	Simulação de mensagens (por exemplo, mensagens de perceção cooperativa ou coordenação de manobras entre o veículo e o ambiente — V2X, mensagens GNSS, etc.) por disfarce de identidade pessoal	M10	O veículo deve verificar a autenticidade e a integridade das mensagens que recebe
4.2	Ataque Sybil (visando simular outros veículos para fazer crer que há muitos na estrada)	M11	Devem ser realizados controlos de segurança para armazenar chaves criptográficas (por exemplo, utilização de módulos de segurança de *hardware*)
5.1	Os canais de comunicação permitem a injeção de código nos dados ou no código do veículo, por exemplo, um código binário de *software* manipulado pode ser injetado no fluxo de comunicação	M10 M6	O veículo deve verificar a autenticidade e a integridade das mensagens que recebe Os sistemas devem garantir a segurança desde a conceção, a fim de minimizar os riscos
5.2	Os canais de comunicação permitem a manipulação dos dados ou do código do veículo	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema
5.3	Os canais de comunicação permitem substituir os dados ou o código do veículo		
5.4 21.1	Os canais de comunicação permitem suprimir os dados ou o código do veículo		
5.5	Os canais de comunicação permitem a introdução de dados ou de código nos sistemas do veículo (escrever o código ou dados)		

Referência do quadro A1	Ameaças aos «canais de comunicação dos veículos»	Ref	Medidas de mitigação
6.1	Aceitação de informações provenientes de uma fonte não fiável	M10	O veículo deve verificar a autenticidade e a integridade das mensagens que recebe
6.2	Ataque de homem no meio (comunicação intercetada)/ sequestro de sessão	M10	O veículo deve verificar a autenticidade e a integridade das mensagens que recebe
6.3	Ataque de replicação, por exemplo um ataque contra um portal de comunicação permite ao atacante instalar uma versão anterior do *software* de uma UCE ou de um microprograma (*firmware*) do portal		
7.1	Interceção de informações/ radiações perturbadoras/ monitorização de comunicações	M12	Os dados confidenciais recebidos ou transmitidos pelo veículo devem estar protegidos.
7.2	Obtenção de acesso não autorizado a ficheiros ou dados	M8	A conceção do sistema e o controlo do acesso deveriam impedir que pessoas não autorizadas possam aceder a dados pessoais ou a dados críticos do sistema. Para exemplos de controlos de segurança, ver o OWASP.
8.1	Envio de um grande número de dados parasitas ao sistema de informação do veículo, de modo a que este seja incapaz de prestar os serviços normalmente	M13	Devem ser aplicadas medidas para detetar e recuperar de um ataque de negação de serviço
8.2	Ataque por buraco negro, perturbação da comunicação entre veículos por bloqueio da transferência de mensagens para outros veículos	M13	Devem ser aplicadas medidas para detetar e recuperar de um ataque de negação de serviço
9.1	Um utilizador não privilegiado pode obter um acesso privilegiado, por exemplo, à raiz do sistema	M9	Devem ser aplicadas medidas para prevenir e detetar o acesso não autorizado
10.1	Um vírus incorporado nos meios de comunicação infeta os sistemas do veículo	M14	Devem ser consideradas medidas para proteger os sistemas contra vírus incorporados ou programas maliciosos (*malware*).
11.1	Mensagens internas (por exemplo, CAN) maliciosas	M15	Devem ser consideradas medidas para detetar mensagens ou atividades internas maliciosas
11.2	Mensagens V2X maliciosas, por exemplo, mensagens de infraestrutura para o veículo ou de veículo a veículo (por exemplo, CAM, DENM)	M10	O veículo deve verificar a autenticidade e a integridade das mensagens que recebe
11.3	Mensagens de diagnóstico maliciosas		
11.4	Mensagens proprietárias maliciosas (por exemplo, as normalmente enviadas a partir de OEM ou de fornecedores de componentes/sistemas/funções)		

2. Medidas de mitigação para o «processo de atualização»

As medidas de mitigação das ameaças relacionadas com o «processo de atualização» constam do quadro B2.

Quadro B2

Medidas de mitigação das ameaças relacionadas com o «processo de atualização»

Referência do quadro A1	Ameaças ao «processo de atualização»	Ref	Medidas de mitigação
12.1	Comprometimento dos procedimentos de atualização sem fios do *software*, incluindo o fabrico do programa ou do microprograma (*firmware*) de atualização do sistema	M16	Devem ser aplicados procedimentos seguros de atualização do *software*
12.2	Comprometimento dos procedimentos de atualização locais/físicos do *software*, incluindo o fabrico do programa ou do microprograma (*firmware*) de atualização do sistema		
12.3	O *software* é manipulado antes do processo de atualização (e, por isso, está corrompido), embora o processo de atualização esteja intacto		
12.4	Comprometimento das chaves criptográficas do fornecedor de *software* visando permitir uma atualização não válida	M11	Devem ser realizados controlos de segurança para armazenar chaves criptográficas
13.1	Ataque de negação de serviço contra o servidor ou a rede de atualização para impedir a disponibilização de atualizações de *software* crítico e/ou desbloquear funcionalidades específicas do cliente	M3	Devem ser realizados controlos de segurança aos sistemas de apoio de retaguarda. Nos casos em que os servidores de apoio de retaguarda são críticos para a prestação de serviços, estão disponíveis medidas de recuperação em caso de interrupção do sistema. Para exemplos de controlos de segurança, ver o OWASP

3. Medidas de mitigação para «ações humanas não intencionais que facilitem um ciberataque»

As medidas de mitigação das ameaças relacionadas com «ações humanas não intencionais que facilitem um ciberataque» constam do quadro B3.

Quadro B3

Medidas de mitigação das ameaças relacionadas com «ações humanas não intencionais que facilitem um ciberataque»

Referência do quadro A1	Ameaças relativas a «ações humanas não intencionais»	Ref	Medidas de mitigação
15.1	Vítima inocente (por exemplo, proprietário, operador ou engenheiro de manutenção) enganado e levado a carregar um programa malicioso (*malware*) de forma não intencional ou a permitir um ataque	M18	Devem ser tomadas medidas para definir e controlar os papéis dos utilizadores e os privilégios de acesso, com base no princípio do menor privilégio

Referência do quadro A1	Ameaças relativas a «ações humanas não intencionais»	Ref	Medidas de mitigação
15.2	Os procedimentos de segurança definidos não são seguidos	M19	As organizações devem assegurar que os procedimentos de segurança são definidos e seguidos, incluindo o registo de ações e o acesso relacionado com a gestão das funções de segurança

4. Medidas de mitigação para «conectividade e conexões externas»

As medidas de mitigação das ameaças relacionadas com «conectividade e conexões externas» constam do quadro B4.

Quadro B4

Medidas de mitigação das ameaças relacionadas com «conectividade e conexões externas»

Referência do quadro A1	Ameaças à «conectividade e conexões externas»	Ref	Medidas de mitigação
16.1	Manipulação de funções concebidas para comandar sistemas de veículos à distância, como uma chave remota, um dispositivo de imobilização e um posto de carregamento	M20	Devem ser realizados controlos de segurança a sistemas com acesso remoto
16.2	Manipulação da telemática do veículo (por exemplo, manipulação da medição de temperatura de mercadorias sensíveis, desbloqueio à distância das portas de carga)		
16.3	Interferência com sistemas ou sensores sem fios de curto alcance		
17.1	Utilização de aplicações corrompidas, ou cuja segurança de *software* é deficiente, para atacar sistemas do veículo	M21	O *software* deve ser avaliado em termos de segurança, autenticado e a sua integridade protegida. Devem ser realizados controlos de segurança para minimizar o risco decorrente de *software* de terceiros destinado a ser instalado ou previsivelmente alojado no veículo
18.1	Interfaces externas, tais como portas USB ou outras, utilizadas como ponto de ataque, por exemplo através de injeção de código	M22	Devem ser realizados controlos de segurança às interfaces externas
18.2	Suporte infetado com vírus conectado ao veículo		
18.3	Acesso diagnóstico (por exemplo, dispositivos de conexão à porta OBD) utilizado para facilitar um ataque, por exemplo, manipular (direta ou indiretamente) parâmetros do veículo	M22	Devem ser realizados controlos de segurança às interfaces externas

5. Medidas de mitigação para «potenciais alvos ou motivações de um ataque»

As medidas de mitigação das ameaças relacionadas com «potenciais alvos ou motivações de um ataque» constam do quadro B5.

Quadro B5

Medidas de mitigação das ameaças relacionadas com «potenciais alvos ou motivações de um ataque»

Referência do quadro A1	Ameaças a «potenciais alvos ou motivações de um ataque»	Ref	Medidas de mitigação
19.1	Extração de *software* proprietário ou com direitos de autor dos sistemas do veículo (pirataria de produtos/*software* roubado)	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP
19.2	Acesso não autorizado às informações privadas do proprietário, tais como a sua identidade, contas de pagamento, livro de endereços, informações sobre a sua localização, identificação eletrónica do veículo, etc.	M8	A conceção do sistema e o controlo do acesso deveriam impedir que pessoas não autorizadas possam aceder a dados pessoais ou a dados críticos do sistema. Para exemplos de controlos de segurança, ver o OWASP
19.3	Extração de chaves criptográficas	M11	Devem ser realizados controlos de segurança para armazenar chaves criptográficas, por exemplo módulos de segurança
20.1	Alterações ilícitas/não autorizadas da identificação eletrónica do veículo	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP
20.2	Fraude de identidade. Por exemplo, se um utilizador pretender apresentar outra identidade ao comunicar com os sistemas de portagem, o sistema dorsal do fabricante		
20.3	Medida para contornar os sistemas de monitorização (por exemplo, pirataria informática/manipulação/bloqueio de mensagens, tal como dados de ODR Tracker ou o número de execuções)	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP É possível mitigar os ataques de manipulação de dados contra sensores ou dados transmitidos através da correlação dos dados provenientes de diferentes fontes de informação.
20.4	Manipulação de dados que falsifique os dados de condução do veículo (por exemplo, quilometragem, velocidade de condução, itinerários, etc.)		
20.5	Alterações não autorizadas dos dados de diagnóstico do sistema		
21.1	Supressão/manipulação não autorizada dos registos de eventos do sistema	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP
22.2	Introduzir *software* malicioso ou atividade de *software* malicioso	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP
23.1	Fabrico de *software* do sistema de comando ou de informação do veículo		

Referência do quadro A1	Ameaças a «potenciais alvos ou motivações de um ataque»	Ref	Medidas de mitigação
24.1	Negação de serviço, que pode, por exemplo, ser desencadeada na rede interna, inundando um barramento CAN ou provocando avarias numa UCE através de uma elevada taxa de envio de mensagens	M13	Devem ser aplicadas medidas para detetar e recuperar de um ataque de negação de serviço
25.1	Acesso não autorizado visando falsificar os parâmetros de configuração das funções críticas do veículo, tais como os dados de travagem, o limiar de projeção do saco insuflável (*airbag*), etc.	M7	Devem ser aplicadas técnicas e conceções de controlo do acesso para proteger os dados ou o código do sistema. Para exemplos de controlos de segurança, ver o OWASP
25.2	Acesso não autorizado visando falsificar os parâmetros de carga, tais como a tensão de carga, a potência de carga, a temperatura da bateria, etc.		

6. Medidas de mitigação para «vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas»

As medidas de mitigação das ameaças relacionadas com «vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas» constam do quadro B6.

Quadro B6

Medidas de mitigação das ameaças relacionadas com «vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas»

Referência do quadro A1	Ameaças a «vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas»	Ref	Medidas de mitigação
26.1	A combinação de chaves criptográficas curtas e um longo período de validade permite ao atacante quebrar a cifragem	M23	Devem ser seguidas as melhores práticas em matéria de cibersegurança para o desenvolvimento de *software* e *hardware*
26.2	Recurso insuficiente aos algoritmos criptográficos para proteger os sistemas vulneráveis		
26.3	Utilização de algoritmos criptográficos obsoletos		
27.1	*Hardware* ou *software* concebido para permitir um ataque ou que não cumpre os critérios de conceção para impedir um ataque	M23	Devem ser seguidas as melhores práticas em matéria de cibersegurança para o desenvolvimento de *software* e *hardware*
28.1	A presença de erros de *software* pode constituir uma base para vulnerabilidades suscetíveis de ser exploradas, particularmente se o software não tiver sido testado para verificar a ausência de códigos errados ou de erros conhecidos e para reduzir o risco da presença de outros desconhecidos	M23	Devem ser seguidas as melhores práticas em matéria de cibersegurança para o desenvolvimento de *software* e *hardware*. Os controlos em matéria de cibersegurança devem ter cobertura adequada

Referência do quadro A1	Ameaças a «vulnerabilidades potenciais suscetíveis de ser exploradas se não forem suficientemente protegidas ou reduzidas»	Ref	Medidas de mitigação
28.2	A utilização de restos da fase de desenvolvimento (por exemplo, portas de correção, portas JTAG, microprocessadores, certificados de desenvolvimento, senhas de desenvolvimento, etc.) pode permitir a um atacante o acesso às unidades de controlo eletrónico (UCE) ou obter privilégios mais elevados		
29.1	Portas de Internet supérfluas deixadas abertas, que dão acesso aos sistemas de rede		
29.2	Contornar a separação das redes para obter controlo. Um exemplo específico é a utilização de portais de acesso ou pontos de acesso não protegidos (tais como as portais de acesso de camião-reboque) para contornar as proteções e obter acesso a outros segmentos da rede com vista a cometer atos maliciosos, como o envio de mensagens arbitrárias do barramento CAN	M23	Devem ser seguidas as melhores práticas em matéria de cibersegurança para o desenvolvimento de *software* e *hardware*. Devem ser seguidas as melhores práticas em matéria de cibersegurança para a conceção de sistemas e integração de sistemas

7. Medidas de mitigação para «perda de dados/violação de dados do veículo»

As medidas de mitigação das ameaças relacionadas com a «perda de dados/violação de dados do veículo» constam do quadro B7.

Quadro B7

Medidas de mitigação das ameaças relacionadas com a «perda de dados/violação de dados do veículo»

Referência do quadro A1	Ameaças de «perda de dados/violação de dados do veículo»	Ref	Medidas de mitigação
31.1	Violação de informações. Os dados pessoais podem ser violados quando o automóvel muda de utilizador (por exemplo, em caso de venda ou de utilização como veículo de aluguer por novos clientes)	M24	Devem ser seguidas as melhores práticas para a proteção da integridade e confidencialidade dos dados no armazenamento dos dados pessoais.

8. Medidas de mitigação para a «manipulação física dos sistemas com vista a permitir um ataque»

As medidas de mitigação das ameaças relacionadas com a «manipulação física dos sistemas com vista a permitir um ataque» constam do quadro B8.

Quadro B8

Medidas de mitigação das ameaças relacionadas com a «manipulação física dos sistemas com vista a permitir um ataque»

Referência do quadro A1	Ameaças relacionadas com a «manipulação física dos sistemas com vista a permitir um ataque»	Ref	Medidas de mitigação
32.1	Manipulação do equipamento eletrónico (*hardware* OEM), por exemplo, equipamento eletrónico não autorizado adicionado a um veículo para permitir um ataque de «homem no meio»	M9	Devem ser aplicadas medidas para prevenir e detetar o acesso não autorizado

PARTE C

Medidas de mitigação das ameaças fora dos veículos

1. Medidas de mitigação para «servidores de apoio de retaguarda»

As medidas de mitigação das ameaças relacionadas com os «servidores de apoio de retaguarda» constam do quadro C1.

Quadro C1

Medidas de mitigação das ameaças relacionadas com os «servidores de apoio de retaguarda»

Referência do quadro A1	Ameaças relacionadas com os «servidores de apoio de retaguarda»	Ref	Medidas de mitigação
1.1 e 3.1	Utilização abusiva de privilégios pelo pessoal (ataque interno)	M1	Devem ser realizados controlos de segurança a sistemas de apoio de retaguarda para minimizar o risco de ataque interno.
1.2 e 3.3	Acesso não autorizado ao servidor através da Internet (ativado, por exemplo, por função-alçapão, vulnerabilidades do sistema de *software* não corrigidas, ataques SQL ou outros meios)	M2	Devem ser realizados controlos de segurança a sistemas de apoio de retaguarda para minimizar os acessos não autorizados. Para exemplos de controlos de segurança, ver o OWASP
1.3 e 3.4	Acesso físico não autorizado ao servidor (por meio, por exemplo, de memória USB ou outro suporte de ligação ao servidor)	M8	A conceção do sistema e o controlo do acesso deveriam impedir que pessoas não autorizadas possam aceder a dados pessoais ou a dados críticos do sistema
2.1	Ataque ao servidor de apoio de retaguarda que bloqueia o seu funcionamento, por exemplo, impede-o de interagir com os veículos e de fornecer serviços dos quais dependem	M3	Devem ser realizados controlos de segurança aos sistemas de apoio de retaguarda. Nos casos em que os servidores de apoio de retaguarda são críticos para a prestação de serviços, estão disponíveis medidas de recuperação em caso de interrupção do sistema. Para exemplos de controlos de segurança, ver o OWASP
3.2	Perda de informações na «nuvem». Dados sensíveis podem ser perdidos devido a ataques ou incidentes quando os dados são armazenados por terceiros prestadores de serviços de computação em «nuvem»	M4	Devem ser realizados controlos de segurança para minimizar os riscos associados à computação em nuvem. Para exemplos de controlos de segurança, ver o OWASP e as orientações NCSC sobre computação em nuvem
3.5	Violação de informações através da partilha acidental de dados (por exemplo, erros administrativos, armazenamento dos dados em servidores situados em garagens)	M5	Devem ser realizados controlos de segurança a sistemas de apoio de retaguarda para evitar violações de dados. Para exemplos de controlos de segurança, ver o OWASP

2. Medidas de mitigação para «ações humanas não intencionais»

As medidas de mitigação das ameaças relacionadas com «ações humanas não intencionais» constam do quadro C2.

Quadro C2

Medidas de mitigação das ameaças relacionadas com «ações humanas não intencionais»

Referência do quadro A1	Ameaças relativas a «ações humanas não intencionais»	Ref	Medidas de mitigação
15.1	Vítima inocente (por exemplo, proprietário, operador ou engenheiro de manutenção) enganado e levado a carregar um programa malicioso (*malware*) de forma não intencional ou a permitir um ataque	M18	Devem ser tomadas medidas para definir e controlar os papéis dos utilizadores e os privilégios de acesso, com base no princípio do menor privilégio
15.2	Os procedimentos de segurança definidos não são seguidos	M19	As organizações devem assegurar que os procedimentos de segurança são definidos e seguidos, incluindo o registo de ações e o acesso relacionado com a gestão das funções de segurança

3. Medidas de mitigação para «perda física de dados»

As medidas de mitigação das ameaças relacionadas com a «perda física de dados» constam do quadro C3.

Quadro C3

Medidas de mitigação das ameaças relacionadas com a «perda física de dados»

Referência do quadro A1	Ameaças de «perda física de dados»	Ref	Medidas de mitigação
30.1	Danos causados por terceiros. Dados sensíveis podem ser perdidos ou comprometidos devido a danos físicos em caso de acidente de viação ou de roubo.	M24	Devem ser seguidas as melhores práticas para a proteção da integridade e confidencialidade dos dados no armazenamento dos dados pessoais. Para exemplos de controlos de segurança, ver a ISO/SC27/WG5.
30.2	Perda devido a conflitos de gestão dos direitos digitais (DRM). Os dados do utilizador podem ser suprimidos devido a problemas de DRM.		
30.3	Dados sensíveis (ou a sua integridade) podem perder-se devido ao desgaste dos componentes informáticos, o que pode causar problemas em cascata (em caso de alteração das chaves, por exemplo)		