Conselho da
União Europeia

Bruxelas, 14 de março de 2019
(OR. pt)

7510/19
ADD 4

TRANS 199
DELACT 68

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
data de receção:	13 de março de 2019
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	C(2019) 1789 final - Anexo 4
Assunto:	ANEXO do Regulamento Delegado da Comissão que complementa a Diretiva 2010/40/UE do Parlamento Europeu e do Conselho no que diz respeito à implantação e à utilização operacional de sistemas cooperativos de transporte inteligentes

Envia-se em anexo, à atenção das delegações, o documento C(2019) 1789 final - Anexo 4.

Anexo: C(2019) 1789 final - Anexo 4

COMISSÃO
EUROPEIA

Bruxelas, 13.3.2019
C(2019) 1789 final

ANNEX 4

ANEXO

do

Regulamento Delegado da Comissão

que complementa a Diretiva 2010/40/UE do Parlamento Europeu e do Conselho no que diz respeito à implantação e à utilização operacional de sistemas cooperativos de transporte inteligentes

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

ÍNDICE

1. Política de segurança dos STI-C 2
1.1. Definições e acrónimos 2
1.2. Definições 2
1.3. Estratégia para a segurança da informação 3
1.3.1. Sistemas de gestão da segurança das informações (*Information security management system*, «ISMS») 3
1.4. Classificação das informações 4
1.5. Avaliação do risco 6
1.5.1. Aspetos gerais 6
1.5.2. Critérios de risco para a segurança 6
1.5.2.1. Identificação do risco 6
1.5.2.2. Análise do risco 7
1.5.2.3. Avaliação do risco 8
1.6. Tratamento do risco 8
1.6.1. Aspetos gerais 8
1.6.2. Controlos relativos às estações STI-C 8
1.6.2.1. Controlos genéricos 8
1.6.2.2. Controlos relativos às comunicações entre estações STI-C 8
1.6.2.3. Controlos relativos às estações STI-C enquanto entidades finais 10
1.6.3. Controlos relativos aos participantes no EU CCMS 10
1.7. Conformidade com a presente política de segurança 10
2. Referências 11

ANEXO IV

1. POLÍTICA DE SEGURANÇA DOS STI-C

1.1. Definições e acrónimos

EU CCMS	Sistema de gestão das credenciais de segurança STI-C da União Europeia
CAM	Mensagem de perceção cooperativa (*Cooperative Awareness Message*)
CP	Política de certificação (*Certificate Policy*)
DENM	Mensagem de notificação ambiental descentralizada (*Decentralised Environmental Notification Message*)
ISMS	Sistema de gestão da segurança das informações (*Information Security Management System*)
IVIM	Mensagem infraestrutura-veículo (*Infrastructure-to-Vehicle Information Message*)
SPATEM	Mensagem de fase e temporização de sinal alargadas (*Signal Phase and Timing Extended Message*)
SREM	Mensagem alargada de pedido de sinal (*Signal Request Extended Message*)
SSEM	Mensagem alargada de estado de pedido de sinal (*Signal Request Status Extended Message*)

1.2. Definições

Disponibilidade	Ser acessível e utilizável, mediante pedido de uma entidade autorizada (ISO 27000) [2]
Infraestrutura STI-C	Sistema de instalações, equipamento e aplicações necessários para o funcionamento de uma organização que presta serviços STI-C relacionados a estações STI-C fixas
Partes interessadas nos STI-C	Pessoa, grupo ou organização com um papel e uma responsabilidade na rede STI-C
Informações confidenciais	Informações que não devem ser disponibilizadas ou divulgadas a pessoas, entidades ou processos não autorizados (ISO 27000) [2]
Segurança da informação	Preservação da confidencialidade, integridade e disponibilidade das informações (ISO 27000) [2]
Incidente de segurança da informação	Um evento indesejado ou inesperado de segurança da informação, ou uma série de eventos, com probabilidade significativa de comprometer as operações comerciais e ameaçar a segurança da informação
Integridade	Propriedade de exatidão e exaustividade (ISO 27000) [2]

Mapa local dinâmico (*Local Dynamic Map*, «LDM»)	Um repositório de dados de atualização dinâmica de uma estação STI-C de bordo, relativo às condições locais de condução; inclui informações recebida de sensores de bordo e de mensagens CAM e DENM (ETSI TR 102 893) [5]
Controlo do protocolo	Os instrumentos de controlo do protocolo selecionam o protocolo de transferência de mensagens adequado para um pedido de mensagem enviado e enviam a mensagem às camadas inferiores da pilha de protocolos, num formato que pode ser processado por essas camadas. As mensagens recebidas são convertidas num formato que pode ser tratado no âmbito da estação STI-C e transferido para o instrumento funcional pertinente, para posterior processamento (ETSI TR 102 893) [5]

1.3. Estratégia para a segurança da informação

1.3.1. Sistema de gestão da segurança das informações (Information security management system, «ISMS»)

(1) Cada operador de estação STI-C deve gerir um ISMS em conformidade com a norma ISO/IEC 27001 e com as restrições e os requisitos adicionais estabelecidos na presente secção.

(2) Cada operador de estação STI-C deve determinar as questões externas e internas pertinentes para a estação STI-C, incluindo:

- COM(2016) 766 final [10],
- o RGPD (Regulamento Geral sobre a Proteção de Dados) [6].

(3) Cada operador de estação STI-C deve determinar as partes pertinentes para o ISMS e respetivos requisitos, incluindo todas as partes interessadas nos STI-C.

(4) O âmbito do ISMS deve incluir todas as estações STI-C exploradas e todos os outros sistemas de processamento da informação que processam dados STI-C sob a forma de mensagens STI-C conformes às seguintes normas:

- CAM [7]
- DENM [8]
- IVIM [9]
- SPATEM [9]
- MAPEM [9]
- SSEM [9]
- SREM [9]

(5) Cada operador de estação STI-C deve assegurar que a sua política de segurança da informação é coerente com a presente política.

(6) Cada operador de estação STI-C deve assegurar que os seus objetivos de segurança da informação incluem e são coerentes com os objetivos de segurança e os requisitos de alto nível da presente política.

(7) Os operadores de estação STI-C devem classificar as informações referidas na secção 1.4.

(8) Os operadores de estações STI-C devem aplicar o processo de avaliação do risco de segurança da informação, tal como estabelecido na secção 1.5, periodicamente ou quando forem propostas ou ocorrerem alterações significativas.

(9) Os operadores de estações STI-C e/ou os fabricantes de estações STI-C devem determinar os requisitos de atenuação dos riscos de segurança identificados no processo de avaliação do risco de segurança da informação, em consonância com a secção 1.6.

(10) Os fabricantes de estações STI-C devem conceber, desenvolver e avaliar as estações STI-C e outros sistemas de processamento da informação, de modo a assegurar que estes cumprem os requisitos aplicáveis.

(11) Os operadores de estações STI-C devem explorar as estações STI-C e todos os outros sistemas de processamento da informação que apliquem controlos adequados do risco em matéria de segurança da informação, em conformidade com a secção 1.6.

1.4. Classificação da informação

A presente secção estabelece os requisitos mínimos para a classificação da informação. Tal não impede que as partes interessadas nos STI-C apliquem requisitos mais rigorosos.

(12) Os operadores de estações STI-C devem classificar a informação tratada em categorias de segurança que podem ser representadas como se segue:

Categoria de segurança da informação = {(confidencialidade, impacto), (integridade, impacto), (disponibilidade, impacto)};

(13) As partes interessadas nos STI-C devem classificar a informação gerida em sistemas de categorias de segurança que podem ser representados como se segue:

Sistema de categorias de segurança da informação = {(confidencialidade, impacto), (integridade, impacto), (disponibilidade, impacto)};

(14) Os valores aceitáveis para o impacto potencial são baixo, moderado e elevado, tal como resumido no quadro **1**.

Quadro 1: «Definições de impacto potencial» para cada objetivo de segurança, no que respeita a confidencialidade, integridade e disponibilidade

	Impacto potencial		
Objetivo de segurança	**BAIXO**	**MODERADO**	**ELEVADO**
Confidencialidade Preservar as restrições autorizadas em matéria de acesso e divulgação da informação, incluindo meios de proteção da privacidade pessoal e da informação protegida	A divulgação não autorizada da informação poderá ter um efeito adverso **limitado** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A divulgação não autorizada da informação poderá ter um efeito adverso **grave** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A divulgação não autorizada da informação poderá ter um efeito adverso **grave ou catastrófico** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.

	Impacto potencial		
Integridade Proteger contra a modificação ou destruição indevida da informação; tal inclui garantir a não repudiação e a autenticidade da informação	A modificação ou destruição não autorizadas da informação poderão ter um efeito adverso **limitado** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A modificação ou destruição não autorizadas da informação poderão ter um efeito adverso **grave** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A modificação ou destruição não autorizadas da informação poderão ter um efeito adverso **grave ou catastrófico** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.
Disponibilidade Garantir o acesso e a utilização atempados e fiáveis à informação	A perturbação do acesso ou da utilização da informação ou de um sistema de informação poderão ter um efeito negativo **limitado** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A perturbação do acesso ou da utilização da informação ou de um sistema de informação poderão ter um efeito negativo **grave** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.	A perturbação do acesso ou da utilização da informação ou de um sistema de informação poderão ter um efeito negativo **grave ou catastrófico** nas operações organizacionais, nos ativos organizacionais ou nas pessoas.

(15) Os seguintes tipos de impacto da classificação da informação devem ser considerados em termos do grau de danos ou custos para os serviços STI-C e as partes interessadas nos STI-C causados por um incidente de segurança da informação:

- segurança rodoviária — quando o impacto coloca os utentes da estrada em risco iminente de ferimentos,
- segurança — quando o impacto coloca qualquer uma das partes interessadas nos STI-C em risco iminente de ferimentos,
- impactos operacionais — quando o impacto na eficiência do tráfego rodoviário é substancialmente negativo, ou outro impacto societal, como a pegada ambiental e a criminalidade organizada,
- jurídico — quando o impacto resulta numa ação de conformidade jurídica e/ou regulamentar significativa contra uma ou mais partes interessadas nos STI-C,
- financeiro — quando o impacto resulta em custos monetários diretos ou indiretos para uma ou mais partes interessadas nos STI-C,
- privacidade — impacto jurídico e financeiro do RGPD,
- reputação — quando o impacto resulta em danos para a reputação de uma ou mais partes interessadas nos STI-C e/ou na rede STI-C, por exemplo, cobertura mediática negativa e/ou grande pressão política a nível nacional ou internacional.

(16) As partes interessadas nos STI-C devem respeitar os valores de impacto mínimos que se seguem nas informações tratadas:

Quadro 2: Impactos

	Informação proveniente de estações STI-C fixas	Informação proveniente de estações STI-C móveis
Confidencialidade	CAM: baixo DENM: baixo IVIM: baixo MAPEM: baixo SPATEM: baixo SSEM: baixo	CAM: baixo DENM: baixo SREM: baixo Dados pessoais contidos em qualquer uma das três mensagens: moderado
Integridade	CAM: moderado DENM: moderado IVIM: moderado MAPEM: moderado SPATEM: moderado SSEM: moderado	CAM: moderado DENM: moderado SREM: moderado
Disponibilidade	CAM: baixo DENM: baixo IVIM: baixo MAPEM: baixo SPATEM: baixo SSEM: moderado	CAM: baixo DENM: baixo SREM: moderado

1.5. Avaliação do risco

1.5.1. Aspetos gerais

(17) A avaliação do risco deve ser efetuada periodicamente em conformidade com a norma ISO/IEC 27005. Deve incluir documentação adequada sobre:

- o âmbito da avaliação do risco, ou seja, o sistema avaliado, respetivos limites e finalidade, e a informação que é tratada,
- critérios de risco para a segurança,
- avaliação do risco, incluindo identificação, análise e avaliação.

1.5.2. Critérios de risco para a segurança

(18) Os critérios de avaliação do risco devem ser determinados tendo em conta os seguintes aspetos:

- o valor estratégico do serviço STI-C e da rede STI-C para todas as partes interessadas nos STI-C,
- o valor estratégico do serviço STI-C e da rede STI-C para o operador da estação STI-C do serviço,
- as consequências para a reputação da rede STI-C,
- os requisitos jurídicos e regulamentares, e as obrigações contratuais.

(19) Os critérios de impacto do risco devem ser determinados à luz dos tipos de impacto da classificação da informação referidos na secção 1.4.

(20) Os critérios de aceitação do risco devem incluir a identificação dos níveis do risco inaceitáveis para os serviços STI-C e as partes interessadas nos STI-C, por tipo de impacto.

1.5.2.1. Identificação do risco

(21) Os riscos devem ser identificados em conformidade com a norma ISO/IEC 27005. Aplicam-se os seguintes requisitos mínimos:

- os principais ativos a proteger são as mensagens STI-C referidas na secção 1.3.1,
- os ativos de apoio devem ser identificados, incluindo:
  - informação utilizada nas mensagens STI-C (por exemplo, mapa local dinâmico, hora, controlo do protocolo, etc.),
  - as estações STI-C e os seus software, dados de configuração e canais de comunicação associados,
  - ativos de controlo de STI-C centrais,
  - todas as entidades do EU CCMS,
- as ameaças a esses ativos e respetivas fontes devem ser identificadas,
- os controlos existentes e previstos devem ser identificados,
- as vulnerabilidades que possam ser exploradas por ameaças, a fim de causar danos aos ativos ou às partes interessadas nos STI-C devem ser identificadas e descritas como cenários de incidentes,
- as eventuais consequências de incidentes de segurança nos ativos devem ser identificadas com base na classificação da informação.

1.5.2.2. Análise do risco

(22) Aplicam-se os seguintes requisitos mínimos à análise de risco:

- o impacto dos incidentes de segurança da informação identificados nos serviços STI-C e nas partes interessadas nos STI-C deve ser avaliado com base na informação e na categoria de segurança do sistema de informação, utilizando, pelo menos, os três níveis estabelecidos na secção 1.4,
- os níveis de impacto devem ser identificados no que respeita:
  - à totalidade da rede/dos serviços STI-C existentes, e
  - a uma parte interessada/entidade organizacional nos STI-C individual,
- o nível mais elevado será considerado como o impacto total,
- a probabilidade de ocorrência dos cenários de incidentes identificados deve ser avaliada utilizando, pelo menos, os três níveis seguintes:

- improvável (valor 1) — o cenário de incidente não é suscetível de ocorrer/difícil de executar ou a motivação para a intrusão é muito baixa,
- possível (valor 2) — o cenário de incidente pode ocorrer/ser executado ou a motivação para a intrusão é razoável,
- provável (valor 3) — o cenário do incidente é suscetível de ocorrer/fácil de executar e a motivação para a intrusão é elevada,

- os níveis de risco devem ser determinados para todos os cenários de incidente identificados, com base no impacto e na probabilidade do produto, de que resultam pelo menos os seguintes níveis de risco: baixo (valores 1,2), moderado (valores 3,4) e elevado (valores 6,9), definidos do seguinte modo:

Quadro 3: Níveis de risco

Níveis de risco enquanto produto do impacto e da probabilidade		**Probabilidade**		
		improvável (1)	**possível (2)**	**provável (3)**
Impacto	**baixo (1)**	baixo (1)	baixo (2)	moderado (3)
	moderado (2)	baixo (2)	moderado (4)	elevado (6)
	elevado (3)	moderado (3)	elevado (6)	elevado (9)

1.5.2.3. Avaliação do risco

(23) Os níveis de risco devem ser comparados com critérios de avaliação do risco e critérios de aceitação do risco, a fim de determinar quais os riscos que devem ser sujeitos a tratamento. Devem ser tratados, pelo menos, os riscos de nível moderado ou elevado aplicáveis aos serviços STI-C e à rede STI-C, em conformidade com a secção 1.6.

1.6. Tratamento do risco

1.6.1. Aspetos gerais

(24) Os riscos devem ser tratados de uma das seguintes formas:

- a alteração do risco através da utilização dos controlos identificados nas secções 1.6.2 ou 1.6.3, de modo a que o risco residual possa ser reavaliado como aceitável,
- retenção de risco (quando o nível de risco cumpre os critérios de aceitação do risco),
- prevenção do risco.

(25) A partilha ou transferência do risco não é permitida para riscos para a rede STI-C.

(26) O tratamento de risco deve ser documentado e incluir:

- a declaração de aplicabilidade em conformidade com a norma ISO 27001, que estabelece os controlos necessários e determina:
  - a probabilidade residual de ocorrência,

- a gravidade residual do impacto,
- o nível de risco residual,
- as razões da retenção ou da prevenção dos riscos.

1.6.2. Controlos relativos às estações STI-C

1.6.2.1. Controlos genéricos

(27) As estações STI-C devem aplicar contramedidas adequadas para alterar o risco, em conformidade com a secção 1.6.1. Essas contramedidas devem aplicar controlos genéricos, tal como definidos nas normas ISO/IEC 27001 e ISO/IEC 27002.

1.6.2.2. Controlos relativos às comunicações entre estações STI-C

(28) Do lado recetor, devem ser estabelecidos os seguintes controlos obrigatórios mínimos:

Quadro 4: Controlos do lado emissor

	Informação proveniente de estações STI-C fixas	**Informação proveniente de estações STI-C móveis**
Confidencialidade	-	Os dados pessoais contidos nas mensagens devem ser securizados através de um procedimento de alteração CA adequado, a fim de garantir um nível de segurança adequado ao risco de reidentificação dos condutores, com base nos dados que transmitiram. Por conseguinte, as estações STI-C devem alterar os CA de forma adequada, ao enviarem mensagens, e não devem reutilizar CA após uma alteração, exceto nos casos em que os condutores não tenham um comportamento de condução médio[1].
Integridade	Todas as mensagens devem ser assinadas em conformidade com a TS 103 097 [14].	Todas as mensagens devem ser assinadas em conformidade com a TS 103 097 [14].
Disponibilidade	-	-

(29) Do lado recetor, devem ser estabelecidos os seguintes controlos obrigatórios mínimos:

Quadro 5: Controlos do lado recetor

	Informação proveniente de estações STI-C fixas	**Informação proveniente de estações STI-C móveis**

[1] A definição de comportamento de condução médio deve basear-se na análise estatística pertinente do comportamento de condução na União Europeia, por exemplo, com base em dados do Centro Aeroespacial Alemão («DLR»).

Confidencialidade		Os dados pessoais recebidos devem ser conservados por um período tão curto quanto possível, para fins profissionais, durante um **período máximo de retensão de cinco minutos**, no caso dos elementos de dados brutos e identificáveis. Uma CAM ou SRM recebidas não devem ser transmitidas/divulgadas. Uma DENM recebida só pode ser transmitida/divulgada numa zona geográfica limitada.
Integridade	A integridade de todas as mensagens utilizadas pelas aplicações STI deve ser validada em conformidade com a norma TS 103 097 [14].	A integridade de todas as mensagens utilizadas pelas aplicações STI deve ser validada em conformidade com a norma TS 103 097 [14].
Disponibilidade	-	As SRM recebidas devem ser processadas e produzir uma emissão SSM para o remetente da SMR.

(30) A fim de apoiar os requisitos de segurança em matéria de confidencialidade, integridade e disponibilidade estabelecidos nos quadros *supra*, todas as estações STI-C [estações de STI-C móveis (incluindo estações STI-C de bordo) e estações STI-C fixas] devem ser avaliadas e certificadas utilizando os critérios de avaliação da segurança especificados nos «Critérios Comuns»/na norma ISO 15408[2]. Devido às diferentes características dos diferentes tipos de estações STI-C e aos diferentes requisitos de privacidade de localização, podem ser definidos perfis de proteção diferentes.

(31) Todos os perfis de proteção e documentos conexos aplicáveis para a certificação de segurança das estações STI-C devem ser avaliados, validados e certificados em conformidade com a norma ISO 15408, aplicando o *Acordo de Reconhecimento Mútuo de Certificados de Avaliação da Segurança da Tecnologia da Informação* do Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS)[3] ou um sistema europeu de certificação da cibersegurança equivalente ao abrigo do quadro europeu de cibersegurança pertinente. Ao desenvolver esses perfis de proteção, o âmbito da certificação de segurança da estação STI-C pode ser definido pelo fabricante, sob reserva da avaliação e da aprovação da CPA e de um organismo de avaliação da conformidade SOG-IS ou, pelo menos, equivalente, como descrito no parágrafo que se segue.

(32) Dada a importância de manter o nível de segurança mais elevado possível, os certificados de segurança das estações STI-C devem ser emitidos ao abrigo do regime de certificação de critérios comuns (ISO 15408) por um organismo de avaliação da conformidade reconhecido pelo comité de gestão no âmbito do Acordo SOG-IS, ou emitidos por um organismo de avaliação da conformidade

[2] Portal «Critérios Comuns»: http://www.commoncriteriaportal.org/cc/

[3] No setor dos transportes rodoviários, o SOG-IS já esteve envolvido na certificação da segurança do tacógrafo inteligente, por exemplo. O acordo SOG-IS é atualmente o único regime na Europa que pode apoiar a harmonização da certificação de segurança dos produtos eletrónicos. Na presente fase, o SOG-IS apoia apenas o processo relativo aos «Critérios Comuns», pelo que as estações STI-C devem ser avaliadas e certificadas de acordo com os «Critérios Comuns»; ver https://www.sogis.org/

acreditado por uma autoridade nacional de certificação da cibersegurança de um Estado-Membro. Esse organismo de avaliação da conformidade deve fornecer, pelo menos, condições equivalentes de avaliação da segurança às previstas no Acordo de Reconhecimento Mútuo SOG-IS.

1.6.2.3. Controlos relativos às estações STI-C enquanto entidades finais

(33) As estações STI-C devem cumprir a política de certificação [1] em conformidade com o seu papel enquanto entidade final do EU CCMS.

1.6.3. Controlos relativos aos participantes no EU CCMS

(34) Os participantes no EU CCMS devem cumprir a política de certificação [1] em conformidade com o seu papel no EU CCMS.

1.7. Conformidade com a presente política de segurança

(35) Os operadores de estações STI-C devem solicitar periodicamente e obter a certificação da conformidade com a presente política, de acordo com as diretrizes para uma auditoria ISO 27001 em [12].

(36) O organismo de auditoria deve ser acreditado e certificado por um membro da Acreditação Europeia. Deve cumprir os requisitos de [11].

(37) Com o objetivo de obter a certificação, os operadores de estações STI-C devem gerar e manter documentos relativos aos requisitos em matéria de informações documentadas em [3], cláusula 7.5. Em especial, os operadores de estações STI-C devem gerar e conservar os seguintes documentos relacionados com o ISMS:

- âmbito de aplicação do ISMS (secção 1.3.1 e [3], cláusula 4.3),
- política e objetivos em matéria de segurança da informação (secção 1.3.1 e [3], cláusulas 5.2 e 6.2),
- Informações pormenorizadas sobre avaliação do risco e metodologia de tratamento do risco (secção 1.5 e [3], cláusula 6.1.2),
- relatório de avaliação do risco (secção 1.5 e [3], cláusula 8.2),
- declaração de aplicabilidade (secção 1.6 e [3], cláusula 6.1.3d),
- plano de tratamento de risco (secções 1.6 e [3], pontos 6.1.3e e 8.3),
- documentos necessários para a implementação dos controlos selecionados (secção 1.6 e [3], anexo A).

(38) Além disso, os operadores de estações STI-C devem gerar e conservar os seguintes registos como prova dos resultados obtidos:

- registos de formação, competências, experiência e qualificações ([3], cláusula 7.2),
- resultados de monitorização e medição ([3], cláusula 9.1),
- programa de auditoria interna ([3], cláusula 9.2),
- resultados das auditorias internas ([3], cláusula 9.2),
- resultados da análise da gestão ([3], cláusula 9.3),
- resultados das medidas corretivas ([3], cláusula 10.1).

2. REFERÊNCIAS

No presente anexo, utilizam-se as seguintes referências:

[1] Anexo III do presente regulamento

[2] ISO/IEC 27000 (2016): *Information technology – security techniques – information security management systems – overview and vocabulary* (Tecnologias de informação — Técnicas de Segurança — Sistemas de gestão da segurança da informação — Visão geral e vocabulário)

[3] ISO/IEC 27001 (2015): Tecnologias de informação — Técnicas de Segurança — Sistemas de gestão da segurança da informação — Requisitos

[4] ISO/IEC 27005 (2011): *Information technology – security techniques – information security risk management* (Tecnologias de informação — Técnicas de Segurança — Gestão do risco para a segurança da informação)

[5] ETSI TR 102 893 V1.2.1, *Intelligent transport systems (ITS) – security; vulnerability and risk analysis (TVRA)* [Sistemas de transporte inteligentes (STI) — Segurança; análise das ameaças, da vulnerabilidade e do risco (TVRA)]

[6] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

[7] ETSI EN 302 637-2 V1.4.0, *Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications* [Sistemas de transporte inteligentes (STI) — Comunicações em veículos; Conjunto básico de aplicações], *Part 2: Specification of cooperative awareness basic service* (Parte 2: Especificação do serviço básico de perceção cooperativa)

[8] ETSI EN 302 637-3 V1.3.0, *Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications* [Sistemas de transporte inteligentes (STI) — Comunicações em veículos; Conjunto básico de aplicações], *Part 3: Specifications of decentralised environmental notification basic service* (Parte 3: Especificações do serviço básico de notificação ambiental descentralizada)

[9] ETSI TS 103 301 V1.2.1: *Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Facilities layer protocols and communication requirements for infrastructure services* [Sistemas de transporte inteligentes (STI) — Comunicações em veículos; Conjunto básico de aplicações; Protocolos com camada de serviços e requisitos de comunicação aplicáveis aos serviços de infraestrutura]

[10] Uma estratégia europeia relativa aos sistemas cooperativos de transporte inteligentes, uma etapa rumo a uma mobilidade cooperativa, conectada e automatizada [COM(2016) 766 de 30 de novembro de 2016]

[11] ISO/IEC 27006:2015 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information*

security management systems (Tecnologias de Informação — Técnicas de Segurança — Requisitos para organismos que fornecem auditoria e certificação dos sistemas de gestão da segurança da informação)

[12] ISO/IEC 27007:2011 *Information technology — Security techniques — Guidelines for information security management systems auditing* (Tecnologias de Informação — Técnicas de Segurança — Orientações para a auditoria de sistemas de gestão da segurança da informação)

[13] ETSI EN 302 665 V1.1.1 *Intelligent transport systems (ITS); Communications architecture* [Sistemas de transporte inteligentes (ITS); Arquitetura das comunicações]

[14] ETSI TS 103 097 V1.3.1. *Intelligent transport systems (ITS) security; security header and certificate formats* [Segurança dos sistemas de transporte inteligentes (STI); cabeçalho de segurança e formato do certificado]