COMISIÓN
EUROPEA

Bruselas, 13.3.2019
C(2019) 1789 final

ANNEX 4

ANEXO

del

Reglamento Delegado de la Comisión

que complementa la Directiva 2010/40/UE del Parlamento Europeo y del Consejo por lo que respecta a la implantación y el uso operativo de los sistemas de transporte inteligentes cooperativos

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

ÍNDICE

ANEXO IV

1. POLÍTICA DE SEGURIDAD DE LOS STI-C

1.1. Definiciones y acrónimos

CAM	mensaje de concienciación cooperativa (*cooperative awareness message*)
CCMS de la UE	sistema de la UE para la gestión de credenciales de seguridad de los STI-C (*European Union C-ITS security credential management system*)
CP	política de certificación (*certificate policy*)
DENM	mensaje de notificación ambiental descentralizada (*decentralised environmental notification message*)
IVIM	mensaje de información de infraestructura a vehículo (*infrastructure-to-vehicle information message*)
SGSI	sistema de gestión de la seguridad de la información (*information security management system*)
SPATEM	mensaje extendido de fase y temporización de señales (*signal phase and timing extended message*)
SREM	mensaje extendido de petición de señales (*signal request extended message*)
SSEM	mensaje extendido de situación de la petición de señales (*signal request status extended message*)

1.2. Definiciones

disponibilidad	propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada (ISO 27000) [2]
infraestructura STI-C	sistema de instalaciones, equipos y aplicaciones necesarios para el funcionamiento de una organización que presta servicios STI-C relacionados con estaciones STI-C fijas
partes interesadas STI-C	individuo, grupo u organización con una función y una responsabilidad en la red STI-C
información confidencial	información que debe mantenerse inaccesible y no revelarse a individuos, entidades o procesos no autorizados (ISO 27000) [2]

seguridad de la información	preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000) [2]
incidente de seguridad de la información	evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información
integridad	propiedad de exactitud y completitud (ISO 27000) [2]
mapa dinámico local (LDM)	repositorio de datos relativos a las condiciones de conducción local de una estación STI-C vehicular actualizado dinámicamente; incluye información recibida de sensores situados a bordo y de mensajes CAM y DENM (ETSI TR 102 893) [5]
control del protocolo	Los activos de control del protocolo seleccionan un protocolo de transferencia de mensajes adecuado para una petición de mensaje saliente y envían el mensaje a las capas inferiores de la pila de protocolos en un formato que pueda ser procesado por esas capas. Los mensajes entrantes son convertidos a un formato que puede ser manejado en la estación STI-C y pasan al activo funcional pertinente para continuar el procesamiento (ETSI TR 102 893) [5]

1.3. Estrategia para la seguridad de la información

1.3.1. Sistema de gestión de la seguridad de la información (SGSI)

1) Los operadores de estaciones STI-C gestionarán los SGSI de conformidad con la norma ISO/IEC 27001 y con las limitaciones y requisitos adicionales que se establecen en el presente epígrafe.

2) Los operadores de estaciones STI-C determinarán qué documentos, externos e internos, son pertinentes para los STI-C, entre ellos:

- el COM(2016) 766 final [10]
- el Reglamento general de protección de datos [6]

3) Los operadores de estaciones STI-C determinarán qué partes son pertinentes para los SGSI y sus requisitos, incluidas todas las partes interesadas STI-C.

4) El ámbito de aplicación de los SGSI incluirá todas las estaciones STI-C gestionadas y todos los demás sistemas de procesamiento de la información que procesen datos STI-C en forma de mensajes STI-C que cumplan las normas siguientes:

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

- SREM [9]

5) Los operadores de estaciones STI-C velarán por que su política de seguridad de la información sea coherente con la presente política.

6) Los operadores de estaciones STI-C velarán por que sus objetivos de seguridad de la información incluyan los objetivos de seguridad y los requisitos de alto nivel de la presente política y sean coherentes con ellos.

7) Los operadores de estaciones STI-C clasificarán la información que figura en el epígrafe 1.4.

8) Los operadores de estaciones STI-C aplicarán el proceso de evaluación del riesgo de la seguridad de la información establecido en el epígrafe 1.5 a intervalos previstos o cuando se propongan o tengan lugar cambios significativos.

9) Los operadores o los fabricantes de estaciones STI-C determinarán los requisitos para mitigar los riesgos de seguridad detectados en el proceso de evaluación del riesgo de la seguridad de la información, en consonancia con el epígrafe 1.6.

10) Los fabricantes de estaciones STI-C diseñarán, desarrollarán y evaluarán estaciones STI-C y otros sistemas de procesamiento de la información de manera que se garantice el cumplimiento de los requisitos aplicables.

11) Los operadores de estaciones STI-C gestionarán las estaciones STI-C y todos los demás sistemas de procesamiento de la información que ejecuten controles adecuados de tratamiento del riesgo de la seguridad de la información en consonancia con el epígrafe 1.6.

1.4. Clasificación de la información

En el presente epígrafe se establecen los requisitos mínimos para la clasificación de la información. Ello no impide que las partes interesadas STI-C apliquen requisitos más estrictos.

12) Los operadores de estaciones STI-C clasificarán la información manejada; las categorías de seguridad pueden representarse de la manera siguiente:

Información sobre la categoría de seguridad = {(confidencialidad, incidencia), (integridad, incidencia), (disponibilidad, incidencia)}.

13) Las partes interesadas STI-C clasificarán la información gestionada; el sistema de categorías de seguridad puede representarse de la manera siguiente:

Sistema de información sobre la categoría de seguridad = {(confidencialidad, incidencia), (integridad, incidencia), (disponibilidad, incidencia)}.

14) Los valores aceptables para la incidencia potencial son: bajo, moderado y alto, como se resume en el cuadro **1**.

Cuadro 1. Definiciones de la incidencia potencial para cada objetivo de seguridad: confidencialidad, integridad y disponibilidad

	Incidencia potencial		
Objetivo de seguridad	**BAJO**	**MODERADO**	**ALTO**

	Incidencia potencial		
Confidencialidad Preservar las restricciones autorizadas sobre el acceso a la información y la revelación de esta, incluidos medios para la protección de la privacidad personal y la información privada.	Cabe esperar que la revelación no autorizada de información tenga un efecto adverso **limitado** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la revelación no autorizada de información tenga un efecto adverso **grave** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la revelación no autorizada de información tenga un efecto adverso **muy grave o catastrófico** en las operaciones y activos de las organizaciones o en los individuos.
Integridad Proteger frente a la modificación o destrucción inadecuada de la información; esto incluye garantizar el no repudio y la autenticidad.	Cabe esperar que la modificación o destrucción no autorizadas de información tengan un efecto adverso **limitado** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la modificación o destrucción no autorizadas de información tengan un efecto adverso **grave** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la modificación o destrucción no autorizadas de información tengan un efecto adverso **muy grave o catastrófico** en las operaciones y activos de las organizaciones o en los individuos.
Disponibilidad Garantizar el acceso a la información y su utilización de manera oportuna y fiable.	Cabe esperar que la interrupción del acceso a la información o a un sistema de información o de su uso tenga un efecto adverso **limitado** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la interrupción del acceso a la información o a un sistema de información o de su uso tenga un efecto adverso **grave** en las operaciones y activos de las organizaciones o en los individuos.	Cabe esperar que la interrupción del acceso a la información o a un sistema de información o de su uso tenga un efecto adverso **muy grave o catastrófico** en las operaciones y activos de las organizaciones o en los individuos.

15) Los siguientes tipos de incidencia de la clasificación de la información se considerarán con arreglo al grado de daño o coste para el servicio STI-C y para las partes interesadas STI-C derivado de un incidente de seguridad de la información:

- seguridad vial: la incidencia pone a los usuarios de la vía pública en riesgo inminente de lesión;
- seguridad: la incidencia pone a cualquiera de las partes interesadas STI-C en riesgo inminente de lesión;
- incidencias operativas: la incidencia es sustancialmente negativa para la eficiencia del tráfico por carretera, u otra incidencia social, como la huella medioambiental o la delincuencia organizada;
- tipo jurídico: la incidencia da lugar a medidas de conformidad significativas de carácter jurídico o normativo contra una o varias partes interesadas STI-C;
- tipo financiero: la incidencia genera un coste económico para una o varias partes interesadas STI-C;
- privacidad: el Reglamento general de protección de datos tiene incidencia tanto jurídica como financiera;

- reputación: la incidencia causa un daño a la reputación de una o varias partes interesadas STI-C o a la red STI-C; por ejemplo, cobertura negativa en la prensa o importante presión política a escala nacional o internacional.

16) Las partes interesadas STI-C deberán respetar los valores mínimos de incidencia que figuran a continuación con respecto a la información manejada:

Cuadro 2. Incidencia

	Información procedente de estaciones STI-C fijas	**Información procedente de estaciones STI-C móviles**
Confidencialidad	CAM: baja DENM: baja IVIM: baja MAPEM: baja SPATEM: baja SSEM: baja	CAM: baja DENM: baja SREM: baja datos personales contenidos en cualquiera de los tres mensajes: moderada
Integridad	CAM: moderada DENM: moderada IVIM: moderada MAPEM: moderada SPATEM: moderada SSEM: moderada	CAM: moderada DENM: moderada SREM: moderada
Disponibilidad	CAM: baja DENM: baja IVIM: baja MAPEM: baja SPATEM: baja SSEM: moderada	CAM: baja DENM: baja SREM: moderada

1.5. Evaluación del riesgo

1.5.1. Generalidades

17) Se llevarán a cabo periódicamente evaluaciones del riesgo en consonancia con la norma ISO/IEC 27005. Incluirán documentación adecuada sobre:

- el alcance de la evaluación del riesgo, es decir, el sistema que se evalúa y sus límites, así como el propósito del sistema y la información que se maneja;
- criterios relativos a los riesgos de seguridad;
- evaluación del riesgo, incluida la identificación, el análisis y la valoración.

1.5.2. Criterios relativos a los riesgos de seguridad

18) Los criterios para la valoración del riesgo se determinarán teniendo en cuenta los aspectos siguientes:

- el valor estratégico del servicio STI-C y la red STI-C para todas las partes interesadas STI-C;
- el valor estratégico del servicio STI-C y de la red STI-C para el operador del servicio de la estación STI-C;
- las consecuencias para la reputación de la red STI-C;
- los requisitos legales y normativos y las obligaciones contractuales.

19) Los criterios para la incidencia de los riesgos se determinarán a la luz de los tipos de incidencia de la clasificación de la información que figuran en el epígrafe 1.4.

20) Los criterios para la aceptación del riesgo incluirán la identificación de los niveles de riesgo que son inaceptables para el servicio STI-C y para las partes interesadas STI-C, por tipo de incidencia.

1.5.2.1. Identificación de los riesgos

21) Los riesgos se identificarán de conformidad con la norma ISO/IEC 27005. Serán de aplicación los siguientes requisitos mínimos:

- los principales activos que deben protegerse son los mensajes STI-C que figuran en el epígrafe 1.3.1;
- deben identificarse los activos de apoyo, como:
  - la información utilizada en los mensajes STI-C (por ejemplo, el mapa dinámico local, la hora, el control del protocolo, etc.);
  - las estaciones STI-C y su *software*, los datos de configuración y los canales de comunicación asociados;
  - los activos de control de los STI-C centrales;
  - cada una de las entidades del CCMS de la UE;
- deberán identificarse las amenazas a esos activos y su origen;
- deberán identificarse los controles existentes y previstos;
- deberán detectarse las vulnerabilidades que pueden ser aprovechadas por las amenazas para causar un daño a los activos o a las partes interesadas STI-C, y deberán describirse como hipótesis de incidente;
- deberán identificarse las posibles consecuencias de los incidentes de seguridad en los activos a partir de la clasificación de la información.

1.5.2.2. Análisis de riesgos

22) Los siguientes requisitos mínimos se aplicarán a los análisis de riesgos:

- se evaluará la incidencia de los incidentes de seguridad de la información en el servicio STI-C y en las partes interesadas STI-C a partir de la información y de la categoría de seguridad del sistema de información utilizando al menos los tres niveles establecidos en el epígrafe 1.4;

- se identificarán los niveles de incidencia para:
  - el total de las redes / los servicios STI-C existentes; y
  - una entidad organizativa / una parte interesada STI-C individual;
- el nivel más elevado se tomará como la incidencia total;
- la probabilidad de las hipótesis de incidente detectadas se evaluará utilizando al menos los tres niveles siguientes:
  - improbable (valor 1): es improbable que tenga lugar la hipótesis de incidente / es difícil de llevar a cabo o la motivación para un atacante es muy baja;
  - posible (valor 2): la hipótesis de incidente puede tener lugar / es posible llevarla a cabo o la motivación para un atacante es razonable;
  - probable (valor 3): es probable que tenga lugar la hipótesis de incidente / es fácil de llevar a cabo y la motivación para un atacante es alta;
- los niveles de riesgo se determinarán para todas las hipótesis de incidente detectadas, a partir del resultado de la incidencia y la probabilidad, que den lugar, al menos, a los siguientes niveles de riesgo: bajo (valores 1, 2), moderado (valores 3, 4) y alto (valores 6, 9), definidos de la manera siguiente:

Cuadro 3. Niveles de riesgo

Niveles de riesgo según el resultado de la incidencia y la probabilidad		**Probabilidad**		
		improbable (1)	**posible (2)**	**probable (3)**
Incidencia	**baja (1)**	baja (1)	baja (2)	moderada (3)
	moderada (2)	baja (2)	moderada (4)	alta (6)
	alta (3)	moderada (3)	alta (6)	alta (9)

1.5.2.3. Valoración del riesgo

23) Los niveles de riesgo se compararán con los criterios para la valoración del riesgo y los criterios para la aceptación del riesgo, a fin de determinar qué riesgos se someterán a tratamiento. Se tratarán, al menos, los riesgos moderado y alto aplicables al servicio STI-C y a la red STI-C, en consonancia con el epígrafe 1.6.

1.6. Tratamiento del riesgo

1.6.1. Generalidades

24) Los riesgos se tratarán de una de las maneras siguientes:

- modificación del riesgo utilizando los controles establecidos en el epígrafe 1.6.2 o 1.6.3, de manera que el riesgo residual pueda evaluarse de nuevo como aceptable;

- retención del riesgo (cuando el nivel de riesgo cumpla los criterios de aceptación del riesgo);
- evitación del riesgo.

25) No está permitido compartir ni transferir los riesgos para la red STI-C.

26) El tratamiento de los riesgos estará documentado, e incluirá:

- la declaración de aplicabilidad, en consonancia con la norma ISO 27001, en la que se establecerán los controles necesarios y se determinará:
  - la probabilidad residual de que ocurra;
  - la gravedad residual de la incidencia;
  - el nivel de riesgo residual;
- las razones para la retención o la evitación del riesgo.

1.6.2. Controles de las estaciones STI-C

1.6.2.1. Controles genéricos

27) Las estaciones STI-C aplicarán contramedidas adecuadas para modificar el riesgo, en consonancia con el epígrafe 1.6.1. Estas contramedidas conllevarán los controles genéricos que se definen en las normas ISO/IEC 27001 e ISO/IEC 27002.

1.6.2.2. Controles de la comunicación entre estaciones STI-C

28) En el lado del emisor se llevarán a cabo los siguientes controles obligatorios mínimos:

Cuadro 4. Controles en el lado del emisor

	Información procedente de estaciones STI-C fijas	**Información procedente de estaciones STI-C móviles**
Confidencialidad	-	Los datos personales contenidos en los mensajes se protegerán por medio de un procedimiento de cambio de AT adecuado, a fin de garantizar un nivel de seguridad oportuno para el riesgo de reidentificación de los conductores a partir de los datos difundidos. Por tanto, las estaciones STI-C cambiarán adecuadamente los AT cuando envíen mensajes y no reutilizarán esos AT después del cambio, excepto en los casos en que el comportamiento del conductor no se ajuste a la media[1].
Integridad	Todos los mensajes irán firmados de conformidad con la TS 103 097 [14].	Todos los mensajes irán firmados de conformidad con la TS 103 097 [14].
Disponibilidad	-	-

[1] La definición de comportamiento de conducción medio se basará en análisis estadísticos pertinentes del comportamiento al volante en la Unión Europea; por ejemplo, basado en datos del Centro Aeroespacial de Alemania.

29) En el lado del receptor se llevarán a cabo los siguientes controles obligatorios mínimos:

Cuadro 5. Controles en el lado del receptor

	Información procedente de estaciones STI-C fijas	**Información procedente de estaciones STI-C móviles**
Confidencialidad		Los datos personales recibidos deben conservarse el menor tiempo posible con fines comerciales, y se establece un **tiempo de conservación máximo de cinco minutos** para los datos en bruto e identificables. Los CAM o SRM recibidos no se reenviarán ni se difundirán. Los DENM recibidos solo podrán reenviarse/difundirse dentro de una zona geográfica limitada.
Integridad	La integridad de todos los mensajes utilizados por las aplicaciones STI se validará de conformidad con la TS 103 097 [14].	La integridad de todos los mensajes utilizados por las aplicaciones STI se validará de conformidad con la TS 103 097 [14].
Disponibilidad	-	Los SRM que se reciban se procesarán, y generarán una difusión de SSM para el remitente del SRM.

30) En apoyo de los requisitos de seguridad [confidencialidad, integridad y disponibilidad] establecidos en los cuadros anteriores, se evaluarán todas las estaciones STI-C (estaciones móviles [incluidas las estaciones STI-C vehiculares] y estaciones fijas) y se certificarán con arreglo a los criterios de evaluación de la seguridad especificados en los «criterios comunes» / ISO 15408[2]. Habida cuenta de las diferentes características de los distintos tipos de estación STI-C y los diferentes requisitos de privacidad de la ubicación, pueden definirse diferentes perfiles de protección.

31) Todos los perfiles de protección y documentos relacionados aplicables para la certificación de la seguridad de las estaciones STI-C se evaluarán, validarán y certificarán en consonancia con la norma ISO 15408, aplicando el Acuerdo sobre el reconocimiento mutuo de certificados de evaluación de la seguridad de las tecnologías de la información del Grupo de Altos Funcionarios sobre Seguridad de los Sistemas de Información (SOG-IS)[3] o un programa europeo de certificación de la ciberseguridad equivalente en el marco europeo de la ciberseguridad pertinente. Para el desarrollo de los perfiles de protección, el fabricante puede definir el alcance de la certificación de la seguridad de la estación STI-C, previa evaluación y aprobación por parte de la CPA y de un

[2] Portal «criterios comunes»: http://www.commoncriteriaportal.org/cc/

[3] En el sector del transporte por carretera, SOG-IS ya ha participado en la certificación de la seguridad de los tacógrafos inteligentes, por ejemplo. El Acuerdo de SOG-IS es, en la actualidad, el único programa europeo en el que puede basarse la armonización de la certificación de la seguridad de los productos electrónicos. Por el momento, SOG-IS solo respalda el proceso de «criterios comunes», por lo que las estaciones STI-C deben evaluarse y configurarse en consonancia con dicho proceso; véase https://www.sogis.org/

organismo de evaluación de la conformidad de SOG-IS, o al menos equivalente, como se describe en el apartado siguiente.

32) Dada la importancia de mantener el nivel de seguridad más elevado posible, los certificados de seguridad para las estaciones STI-C deberá emitirlos, con arreglo al programa de certificación de criterios comunes (ISO 15408), un organismo de evaluación de la conformidad reconocido por el comité de gestión en el marco del Acuerdo SOG-IS o un organismo de evaluación de la conformidad acreditado por una autoridad nacional de certificación de la ciberseguridad de un Estado miembro. El organismo de evaluación de la conformidad deberá proporcionar, al menos, unas condiciones de evaluación de la seguridad equivalentes a las previstas en el Acuerdo sobre el reconocimiento mutuo de SOG-IS.

1.6.2.3. Controles de las estaciones STI-C como entidad final

33) Las estaciones STI-C deberán ser conformes con la política de certificación [1] según su función de entidad final en el CCMS de la UE.

1.6.3. Controles de los participantes en el CCMS de la UE

34) Los participantes en el CCMS de la UE deberán cumplir la política de certificación [1] según la función que desempeñen en dicho sistema.

1.7. Conformidad con la política de seguridad

35) Los operadores de estaciones STI-C deberán solicitar y obtener periódicamente un certificado de conformidad con la presente política con arreglo a las directrices de auditoría de la norma ISO 27001 [12].

36) El organismo de auditoría estará acreditado y certificado por un miembro de la acreditación europea. Deberá cumplir los requisitos de la norma [11].

37) Con el objetivo de obtener la certificación, los operadores de estaciones STI-C generarán y conservarán documentos en los que se aborden los requisitos sobre la información documentada de la norma [3], apartado 7.5. En particular, los operadores de estaciones STI-C generarán y conservarán los documentos siguientes relacionados con los SGSI:

- alcance del SGSI (punto 1.3.1 y [3], apartado 4.3);
- política y objetivos de seguridad de la información (punto 1.3.1 y [3], apartados 5.2 y 6.2);
- información sobre la metodología de evaluación y tratamiento del riesgo (epígrafe 1.5 y [3], apartado 6.1.2);
- informe de evaluación del riesgo (epígrafe 1.5 y [3], apartado 8.2);
- declaración de aplicabilidad (epígrafe 1.6 y [3], apartado 6.1.3.d);
- plan de tratamiento de riesgos (epígrafe 1.6 y [3], apartados 6.1.3.e y 8.3);
- documentos exigidos para llevar a cabo los controles seleccionados (epígrafe 1.6 y [3], anexo A).

38) Además, los operadores de estaciones STI-C generarán y conservarán la documentación siguiente como prueba de los resultados obtenidos:

- justificantes de formación, competencia, experiencia y educación ([3], apartado 7.2);
- resultados de seguimiento y medición ([3], apartado 9.1);
- programa de auditoría interna ([3], apartado 9.2);
- resultados de las auditorías internas ([3], apartado 9.2);
- resultados de la revisión por la dirección ([3], apartado 9.3);
- resultados de las acciones correctivas ([3], apartado 10.1).

2. REFERENCIAS

En el presente anexo se utilizan las referencias siguientes:

[1] Anexo III del presente Reglamento.

[2] ISO/IEC 27000:2016, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Visión de conjunto y vocabulario.

[3] ISO/IEC 27001:2015, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

[4] ISO/IEC 27005:2011, Tecnología de la información. Técnicas de seguridad. Gestión de Riesgos de la Seguridad de la Información.

[5] ETSI TR 102 893 V1.2.1, *Intelligent transport systems (ITS) – security; threat, vulnerability and risk analysis (TVRA)* [sistemas de transporte inteligentes (STI); análisis de amenazas, vulnerabilidad y riesgos]

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[7] ETSI EN 302 637-2 V1.4.0, *Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 2: Specification of cooperative awareness basic service* [sistemas de transporte inteligentes (STI); comunicaciones vehiculares; conjunto básico de aplicaciones; parte 2: especificación del servicio básico de concienciación cooperativa]

[8] ETSI EN 302 637-3 V1.3.0, *Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 3: Specifications of decentralised environmental notification basic service* [sistemas de transporte inteligentes (STI); comunicaciones vehiculares; conjunto básico de aplicaciones; parte 3: especificaciones del servicio básico de notificación 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). Comunicaciones vehiculares. Conjunto básico de aplicaciones. Protocolos de la capa de recursos y requisitos de comunicación para los servicios de infraestructura]

[10] Estrategia europea sobre los sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada [COM(2016) 766, de 30 de noviembre de 2016]

[11] ISO/IEC 27006:2015, Tecnología de la información. Técnicas de seguridad. Requisitos para los organismos que realizan la auditoría y certificación de sistemas de información de gestión de la seguridad

[12] ISO/IEC 27007:2011, Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de sistemas de gestión de la seguridad de la información

[13] ETSI EN 302 665 V1.1.1, *Intelligent transport systems (ITS); Communications architecture* [sistemas de transporte inteligentes (STI); arquitectura de las comunicaciones]

[14] ETSI TS 103 097 V1.3.1, *Intelligent transport systems (ITS) security; security header and certificate formats* [Sistemas de transporte inteligentes (STI). Seguridad. Formatos de cabecera de seguridad y certificados]