COMMISSIONE
EUROPEA

Bruxelles, 13.3.2019
C(2019) 1789 final

ANNEX 4

ALLEGATO

del

regolamento delegato (UE) .../... della Commissione

che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio per quanto riguarda la diffusione e l'utilizzo operativo di sistemi di trasporto intelligenti cooperativi

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

INDICE

ALLEGATO IV

1. POLITICA DI SICUREZZA DEI C-ITS

1.1. Definizioni e acronimi

EU CCMS	Sistema dell'Unione europea di gestione delle credenziali di sicurezza C-ITS
CAM	Messaggio consapevolezza cooperativa (Cooperative Awareness Message)
CP	Politica di certificazione
DENM	Messaggio di notifica di sicurezza decentralizzata innescata da eventi (Decentralized Environmental Notification Message)
SGSI	Sistema di gestione della sicurezza delle informazioni
IVIM	Messaggio di informazione da infrastruttura a veicolo (Infrastructure to Vehicle Information Message)
SPATEM	Messaggio esteso di fase e temporizzazione del segnale (Signal Phase and Timing Extended Message)
SREM	Messaggio esteso di richiesta di segnale (Signal Request Extended Message)
SSEM	Messaggio esteso di status di richiesta di segnale (Signal Request Extended Message)

1.2. Definizioni

Disponibilità	L'essere accessibile e utilizzabile dietro richiesta di un'entità autorizzata (ISO 27000) [2].
Infrastruttura C-ITS	Il sistema degli impianti, delle apparecchiature e delle applicazioni necessari al funzionamento di un'organizzazione che fornisce servizi C-ITS connessi a stazioni C-ITS fisse.
Portatori di interessi nel campo dei C-ITS	Individuo, gruppo od organizzazione avente un ruolo e una responsabilità nella rete C-ITS.
Informazioni riservate	Le informazioni che non devono essere rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO 27000) [2].
Sicurezza delle informazioni	La tutela della riservatezza, dell'integrità e della disponibilità delle informazioni (ISO 27000) [2].
Incidente relativo alla sicurezza delle	Evento o serie di eventi relativi sicurezza delle informazioni non voluti o inattesi che hanno una probabilità significativa di compromettere le attività aziendali e di minacciare la sicurezza delle

informazioni	informazioni.
Integrità	La proprietà dell'essere accurato e completo (ISO 27000) [2].
Mappa dinamica locale (LDM, local dynamic map)	Un repository della stazione C-ITS di bordo aggiornato dinamicamente con i dati relativi alle condizioni di guida locali; comprende le informazioni ricevute dai sensori di bordo e dai messaggi CAM e DENM (ETSI TR 102 893) [5].
Controllo del protocollo	Le risorse di controllo del protocollo selezionano il protocollo di trasferimento di messaggio appropriato per una richiesta di messaggio in uscita e inviano il messaggio ai livelli inferiori dello stack di protocolli in un formato che può essere elaborato da tali livelli. I messaggi in entrata sono convertiti in un formato che può essere gestito nell'ambito della stazione C-ITS e trasferiti alla pertinente risorsa funzionale per un'ulteriore elaborazione (ETSI TR 102 893) [5].

1.3. Strategia per la sicurezza delle informazioni

1.3.1. Sistema di gestione della sicurezza delle informazioni (SGSI)

(1) Ciascun operatore della stazione C-ITS deve gestire un SGSI in conformità alla norma ISO/IEC 27001 e nel rispetto dei vincoli e dei requisiti supplementari stabiliti nella presente sezione.

(2) Ciascun operatore della stazione C-ITS deve determinare le questioni interne ed esterne attinenti ai C-ITS, tenendo conto:

- del COM(2016) 766 final [10];
- del GDPR (regolamento generale sulla protezione dei dati) [6].

(3) Ciascun operatore della stazione C-ITS deve determinare quali parti sono rilevanti per l'SGSI e i relativi requisiti, compresi tutti i portatori di interessi nel campo dei C-ITS.

(4) L'ambito dell'SGSI include tutte le stazioni C-ITS operative e tutti gli altri sistemi di elaborazione delle informazioni che elaborano i dati C-ITS sotto forma di messaggi C-ITS conformi alle seguenti norme:

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

(5) Ciascun operatore della stazione C-ITS deve garantire che le sue politiche in materia di sicurezza delle informazioni siano coerenti con la presente politica.

(6) Ciascun operatore della stazione C-ITS deve garantire che i propri obiettivi in materia di sicurezza delle informazioni includano gli obiettivi di sicurezza e i requisiti di alto livello stabiliti nella presente politica, e siano coerenti con essi.

(7) Gli operatori delle stazioni C-ITS devono classificare le informazioni di cui alla sezione 1.4.

(8) Gli operatori delle stazioni C-ITS devono attuare un processo di valutazione del rischio per la sicurezza delle informazioni di cui alla sezione 1.5 a intervalli pianificati o quando sono proposte o apportate modifiche significative.

(9) Gli operatori delle stazioni C-ITS e/o i fabbricanti delle stazioni C-ITS devono determinare i requisiti per l'attenuazione dei rischi per la sicurezza individuati nel corso della procedura di valutazione del rischio per la sicurezza delle informazioni, in linea con la sezione 1.6.

(10) I fabbricanti delle stazioni C-ITS devono progettare, sviluppare e valutare le stazioni C-ITS e gli altri sistemi di elaborazione delle informazioni in modo da garantire che siano soddisfatti i requisiti applicabili.

(11) Gli operatori delle stazioni C-ITS devono gestire le stazioni C-ITS e tutti gli altri sistemi di elaborazione delle informazioni che attuano adeguati controlli del trattamento del rischio per la sicurezza delle informazioni, in linea con la sezione 1.6.

1.4. Classificazione delle informazioni

La presente sezione stabilisce i requisiti minimi per la classificazione delle informazioni. Ciò non impedisce ai portatori di interessi dei C-ITS di applicare requisiti più rigorosi.

(12) Gli operatori delle stazioni C-ITS devono classificare le informazioni gestite mediante una categoria di sicurezza che può essere così rappresentata:

informazioni relative alla categoria di sicurezza = {(riservatezza, impatto), (integrità, impatto), (disponibilità, impatto)}.

(13) I portatori di interessi nel campo dei C-ITS devono classificare le informazioni gestite mediante una categoria di sicurezza che può essere così rappresentata:

informazioni relative alla categoria di sicurezza del sistema = {(riservatezza, impatto), (integrità, impatto), (disponibilità, impatto)}.

(14) I valori accettabili per l'impatto potenziale sono basso, moderato e alto, come sintetizzato nella tabella **1**.

Tabella 1 - Definizioni dell'impatto potenziale per ciascun obiettivo di sicurezza inerente alla riservatezza, all'integrità e alla disponibilità

	Impatto potenziale		
Obiettivo di sicurezza	**BASSO**	**MODERATO**	**ALTO**
Riservatezza Salvaguardia delle restrizioni autorizzate relative all'accesso e alla divulgazione delle informazioni, comprese le misure che tutelano la vita privata e le informazioni proprietarie.	La divulgazione non autorizzata di informazioni potrebbe avere effetti negativi **limitati** sulle operazioni e sulle risorse organizzative o sui singoli.	La divulgazione non autorizzata di informazioni potrebbe avere effetti negativi **gravi** sulle operazioni e sulle risorse organizzative o sui singoli.	La divulgazione non autorizzata di informazioni potrebbe avere effetti negativi **deleteri o catastrofici** sulle operazioni e sulle risorse organizzative o sui singoli.

	Impatto potenziale		
Integrità Sorveglianza volta ad evitare la modifica o la distruzione inopportune di informazioni; rientra in questo ambito la garanzia di non disconoscibilità e di autenticità delle informazioni.	La modifica o la distruzione non autorizzate di informazioni potrebbe avere effetti negativi **limitati** sulle operazioni e sulle risorse organizzative o sui singoli.	La modifica o la distruzione non autorizzate di informazioni potrebbe avere effetti negativi **gravi** sulle operazioni e sulle risorse organizzative o sui singoli.	La modifica o la distruzione non autorizzate di informazioni potrebbe avere effetti negativi **deleteri o catastrofici** sulle operazioni e sulle risorse organizzative o sui singoli.
Disponibilità Garantire in modo tempestivo e affidabile l'accesso alle informazioni e il loro utilizzo.	L'interruzione dell'accesso alle informazioni o a un sistema di informazione, o del loro rispettivo utilizzo, potrebbe avere effetti negativi **limitati** sulle operazioni e sulle risorse organizzative o sui singoli.	L'interruzione dell'accesso alle informazioni o a un sistema di informazione, o del loro rispettivo utilizzo, potrebbe avere effetti negativi **gravi** sulle operazioni e sulle risorse organizzative o sui singoli.	L'interruzione dell'accesso alle informazioni o a un sistema di informazione, o del loro rispettivo utilizzo, potrebbe avere effetti negativi **deleteri o catastrofici** sulle operazioni e sulle risorse organizzative o sui singoli.

(15) I seguenti tipi d'impatto della classificazione delle informazioni devono essere considerati in base al grado del danno o dei costi, per il servizio C-ITS e per i portatori di interessi nel campo dei C-ITS, causati da un incidente relativo alla sicurezza delle informazioni:

- impatto sulla sicurezza stradale: l'impatto espone gli utenti della strada a un rischio imminente di lesioni;
- impatto sulla sicurezza: l'impatto espone i portatori di interessi nel campo dei C-ITS a un rischio imminente di lesioni;
- impatto di tipo operativo: l'impatto sull'efficienza del traffico stradale è sostanzialmente negativo o si verificano altri tipi di conseguenze di natura sociale, come l'impronta ambientale e la criminalità organizzata;
- impatto di tipo giuridico: l'impatto si traduce in un'importante azione legale in materia di conformità giuridica e/o normativa nei confronti di uno o più portatori di interessi nel campo dei C-ITS;
- impatto di tipo finanziario: l'impatto si traduce in costi monetari diretti o indiretti per uno o più portatori di interessi nel campo dei C-ITS;
- impatto sulla vita privata: il GDPR, che ha un impatto sia giuridico che finanziario;
- impatto sulla reputazione: l'impatto si traduce in un pregiudizio alla reputazione di uno o più portatori di interessi nel campo dei C-ITS e/o della rete C-ITS, ad es. copertura mediatica negativa e/o pressioni politiche rilevanti su scala nazionale o internazionale.

(16) Per le informazioni da loro gestite, i portatori di interessi nel campo dei C-ITS devono rispettare i valori minimi di impatto riportati nella seguente tabella.

Tabella 2 - Impatti

	Informazioni originate da stazioni C-ITS fisse	**Informazioni originate da stazioni C-ITS mobili**
Riservatezza	CAM: basso DENM: basso IVIM: basso MAPEM: basso SPATEM: basso SSEM: basso	CAM: basso DENM: basso SREM: basso dati personali contenuti in uno dei tre messaggi: moderato
Integrità	CAM: moderato DENM: moderato IVIM: moderato MAPEM: moderato SPATEM: moderato SSEM: moderato	CAM: moderato DENM: moderato SREM: moderato
Disponibilità	CAM: basso DENM: basso IVIM: basso MAPEM: basso SPATEM: basso SSEM: moderato	CAM: basso DENM: basso SREM: moderato

1.5. Valutazione del rischio

1.5.1. Aspetti generali

(17) La valutazione del rischio è effettuata periodicamente in linea con la norma ISO/IEC 27005. Tale valutazione deve includere la documentazione pertinente in merito:

- all'ambito della valutazione del rischio, ossia al sistema oggetto della valutazione, ai suoi confini e alle sue finalità, nonché alle informazioni trattate;
- ai criteri di rischio per la sicurezza;
- alla valutazione del rischio, comprese l'individuazione, l'analisi e la valutazione.

1.5.2. Criteri di rischio per la sicurezza

(18) I criteri di valutazione del rischio devono essere determinati tenendo conto dei seguenti aspetti:

- il valore strategico del servizio e della rete C-ITS per tutti i portatori di interessi nel campo dei C-ITS;

- il valore strategico del servizio e della rete C-ITS per l'operatore del servizio della stazione C-ITS;
- le conseguenze sulla reputazione della rete C-ITS;
- gli obblighi giuridici e normativi nonché gli obblighi contrattuali.

(19) I criteri relativi all'impatto del rischio devono essere determinati alla luce dei tipi d'impatto della classificazione delle informazioni di cui alla sezione 1.4.

(20) I criteri di accettazione del rischio devono includere l'individuazione dei livelli di rischio inaccettabili per il servizio C-ITS e per i portatori di interessi nel campo dei C-ITS, specificati per tipo di impatto.

1.5.2.1. Individuazione del rischio

(21) I rischi devono essere individuati conformemente alla norma ISO/IEC 27005. Si applicano i seguenti requisiti minimi:

- le principali risorse da tutelare sono i messaggi C-ITS di cui alla sezione 1.3.1;
- è opportuno individuare risorse di supporto, tra cui:
  - le informazioni utilizzate per i messaggi C-ITS (ad es. mappa dinamica locale, tempo, controllo del protocollo ecc.);
  - le stazioni C-ITS e i relativi software, i dati di configurazione e i canali di comunicazione associati;
  - le risorse centrali di controllo dei C-ITS;
  - tutte le entità nell'ambito dell'EU CCMS;
- occorre individuare le minacce che gravano su tali risorse e l'origine di tali minacce;
- occorre individuare i controlli esistenti e quelli programmati;
- occorre individuare le vulnerabilità che possono essere sfruttate dalle minacce per arrecare un pregiudizio alle risorse o ai portatori di interessi nel campo dei C-ITS; tali vulnerabilità vanno descritte sotto forma di scenari di incidente;
- sulla base della classificazione delle informazioni, occorre individuare le possibili conseguenze degli incidenti di sicurezza sulle risorse.

1.5.2.2. Analisi del rischio

(22) Ai fini dell'analisi del rischio si applicano i seguenti requisiti minimi:

- l'impatto, sul servizio C-ITS e sui portatori di interessi nel campo dei C-ITS, degli incidenti relativi alla sicurezza delle informazioni individuati deve essere valutato sulla base della categoria di sicurezza delle informazioni e del sistema di informazione, utilizzando almeno i tre livelli di cui alla sezione 1.4;
- i livelli di impatto devono essere individuati:
  - per la totalità della rete/dei servizi C-ITS esistenti; e

- per un singolo portatore di interessi/entità organizzativa in ambito C-ITS;

- il livello più alto deve essere considerato come l'impatto complessivo;
- la probabilità degli scenari di incidente individuati deve essere valutata utilizzando almeno i tre livelli seguenti:
  - improbabile (valore 1): il verificarsi dello scenario di incidente è improbabile, la sua realizzazione è difficile o la motivazione dell'utente malintenzionato è molto bassa;
  - possibile (valore 2): lo scenario di incidente può verificarsi, la sua realizzazione è possibile o la motivazione dell'utente malintenzionato è plausibile;
  - probabile (valore 3): il verificarsi dello scenario di incidente è probabile, la sua realizzazione è semplice o la motivazione dell'utente malintenzionato è elevata;
- i livelli di rischio devono essere determinati per tutti gli scenari di incidente individuati sulla base del risultato e della probabilità dell'impatto; ne devono risultare almeno i seguenti livelli di rischio: basso (valori 1 e 2), moderato (valori 3 e 4) e alto (valori 6 e 9), definiti come segue.

Tabella 3 - Livelli di rischio

Livelli di rischio in base all'impatto e alla probabilità		**Probabilità**		
		improbabile (1)	**possibile (2)**	**probabile (3)**
Impatto	**basso (1)**	basso (1)	basso (2)	moderato (3)
	moderato (2)	basso (2)	moderato (4)	alto (6)
	alto (3)	moderato (3)	alto (6)	alto (9)

1.5.2.3. Valutazione del rischio

(23) I livelli di rischio devono essere confrontati con i criteri di valutazione del rischio e con quelli di accettazione del rischio per determinare quali rischi sottoporre a trattamento. Occorre trattare almeno i rischi di livello moderato o alto che possono riguardare il servizio e la rete C-ITS, in linea con la sezione 1.6.

1.6. Trattamento del rischio

1.6.1. Aspetti generali

(24) I rischi devono essere trattati in uno dei seguenti modi:

- modifica del rischio, mediante l'esecuzione dei controlli di cui alla sezione 1.6.2 o 1.6.3, in modo che, ad una nuova valutazione, il rischio residuo possa risultare accettabile;
- mantenimento del rischio (se il livello di rischio soddisfa i criteri di accettazione del rischio);

- prevenzione del rischio.

(25) Non sono consentiti la condivisione o il trasferimento del rischio per i rischi della rete C-ITS.

(26) Il trattamento del rischio deve essere documentato includendo:

- la dichiarazione di applicabilità in linea con la norma ISO 27001, che stabilisce i necessari controlli e determina:
  - la probabilità residua di insorgenza;
  - la gravità residua dell'impatto;
  - il livello di rischio residuo;
- i motivi del mantenimento o della prevenzione del rischio.

1.6.2. Controlli sulle stazioni C-ITS

1.6.2.1. Controlli generici

(27) Le stazioni C-ITS devono mettere in atto contromisure adeguate per modificare il rischio, conformemente alla sezione 1.6.1. Queste contromisure devono attuare controlli generici secondo la definizione delle norme ISO/IEC 27001 e ISO/IEC 27002.

1.6.2.2. Controlli sulla comunicazione tra le stazioni C-ITS

(28) A livello di trasmettitore devono essere attuati i seguenti controlli minimi obbligatori.

Tabella 4 - Controlli a livello di trasmettitore

	Informazioni originate da stazioni C-ITS fisse	**Informazioni originate da stazioni C-ITS mobili**
Riservatezza	-	I dati personali contenuti nei messaggi devono essere protetti utilizzando un'opportuna procedura di modifica dell'AT per garantire un livello di sicurezza adeguato al rischio di re-identificazione dei conducenti sulla base dei dati che hanno trasmesso. Le stazioni C-ITS devono quindi modificare opportunamente l'AT al momento dell'invio dei messaggi e non devono riutilizzare gli AT dopo una modifica, ad eccezione dei casi in cui il conducente ha un comportamento che non rientra nella media[1].
Integrità	Tutti i messaggi devono essere firmati conformemente alla norma TS 103 097 [14].	Tutti i messaggi devono essere firmati conformemente alla norma TS 103 097 [14].
Disponibilità	-	-

(29) A livello di ricevitore devono essere attuati i seguenti controlli minimi obbligatori.

[1] La definizione di comportamento di guida medio deve basarsi su un'analisi statistica pertinente del comportamento di guida nell'Unione europea, basata ad esempio sui dati del Centro aerospaziale tedesco (DLR).

Tabella 5 - Controlli a livello di ricevitore

	Informazioni originate da stazioni C-ITS fisse	Informazioni originate da stazioni C-ITS mobili
Riservatezza		I dati personali ricevuti dovrebbero essere conservati per il minor tempo possibile a fini aziendali, con una **durata massima di conservazione di cinque minuti** per gli elementi dati grezzi e identificabili. Un CAM o un SRM ricevuti non devono essere inoltrati/trasmessi. Un DENM ricevuto può essere inoltrato/trasmesso solo all'interno di un'area geografica limitata.
Integrità	L'integrità di tutti i messaggi utilizzati dalle applicazioni ITS deve essere convalidata conformemente alla norma TS 103 097 [14].	L'integrità di tutti i messaggi utilizzati dalle applicazioni ITS deve essere convalidata conformemente alla norma TS 103 097 [14].
Disponibilità	-	Un SRM ricevuto deve essere elaborato e produrre la trasmissione di un SSM all'iniziatore dell'SRM.

(30) Per supportare i requisiti di sicurezza della riservatezza, dell'integrità e della disponibilità di cui alle tabelle precedenti, tutte le stazioni C-ITS (stazioni C-ITS mobili, comprese le stazioni C-ITS a bordo veicolo, e stazioni C-ITS fisse) devono essere valutate e certificate in base ai criteri di valutazione della sicurezza specificati nei "criteri comuni"/ISO 15408[2]. A causa delle caratteristiche diverse dei vari tipi di stazioni C-ITS e dei diversi requisiti relativi alla tutela della privacy per la posizione, possono essere definiti profili di protezione diversi.

(31) Tutti i profili di protezione e i relativi documenti applicabili per la certificazione di sicurezza delle stazioni C-ITS devono essere valutati, convalidati e certificati in conformità alla norma ISO 15408, applicando l'*Accordo sul reciproco riconoscimento dei certificati di valutazione della sicurezza delle tecnologie dell'informazione* del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (SOG-IS)[3], o a un regime europeo equivalente di certificazione della cibersicurezza nell'ambito del pertinente quadro europeo della cibersicurezza. Nella definizione di tali profili di protezione, l'ambito della certificazione di sicurezza della stazione C-ITS può essere definito dal fabbricante, previa valutazione e approvazione della CPA e di un organismo di valutazione della conformità del SOG-IS o almeno equivalente, come descritto nel paragrafo seguente.

[2] Portale "Criteri comuni": http://www.commoncriteriaportal.org/cc/.

[3] Nel settore dei trasporti su strada, il SOG-IS ha già partecipato, ad esempio, alla certificazione di sicurezza del tachigrafo intelligente. L'accordo SOG-IS è attualmente l'unico regime in Europa in grado di supportare l'armonizzazione della certificazione di sicurezza dei prodotti elettronici. In questa fase, il SOG-IS sostiene solo il processo dei "criteri comuni": pertanto le stazioni C-ITS devono essere valutate e certificate conformemente ai "criteri comuni"; cfr. https://www.sogis.org/.

(32) Data l'importanza di mantenere il massimo livello di sicurezza possibile, i certificati di sicurezza per le stazioni C-ITS devono essere rilasciati nell'ambito del regime di certificazione dei criteri comuni (ISO 15408) da un organismo di valutazione della conformità riconosciuto dal comitato di gestione nel quadro dell'accordo SOG-IS, oppure da un organismo di valutazione della conformità accreditato da un'autorità nazionale di certificazione della cibersicurezza di uno Stato membro. Tale organismo di valutazione della conformità deve fornire condizioni di valutazione della sicurezza almeno equivalenti a quelle previste dall'accordo SOG-IS sul reciproco riconoscimento.

1.6.2.3. Controlli sulle stazioni C-ITS come entità finali

(33) Le stazioni C-ITS devono rispettare la politica di certificazione [1] in funzione del loro ruolo come entità finali dell'EU CCMS.

1.6.3. Controlli sui partecipanti all'EU CCMS

(34) I partecipanti all'EU CCMS devono rispettare la politica di certificazione [1] in funzione del loro ruolo nell'EU CCMS.

1.7. Conformità alla presente politica di sicurezza

(35) Gli operatori delle stazioni C-ITS richiedono e ottengono periodicamente la certificazione di conformità alla presente politica secondo gli orientamenti per un audit ISO 27001 di cui al riferimento [12].

(36) L'organismo di audit deve essere accreditato e certificato da un membro dell'accreditamento europeo. Deve soddisfare i requisiti di cui al riferimento [11].

(37) Allo scopo di ottenere la certificazione, gli operatori delle stazioni C-ITS devono produrre e conservare i documenti relativi ai requisiti sulle informazioni documentate di cui al riferimento [3], clausola 7.5. In particolare gli operatori delle stazioni C-ITS devono produrre e conservare i seguenti documenti relativi all'SGSI:

- l'ambito dell'SGSI (sezione 1.3.1 e [3], clausola 4.3);
- la politica e gli obiettivi della sicurezza delle informazioni (sezione 1.3.1 e [3], clausole 5.2 e 6.2);
- i dettagli relativi alla valutazione del rischio e alla metodologia di trattamento del rischio (sezione 1.5 e [3], clausola 6.1.2);
- la relazione di valutazione del rischio (sezione 1.5 e [3], clausola 8.2);
- la dichiarazione di applicabilità (sezione 1.6 e [3], clausola 6.1.3d);
- il piano di trattamento del rischio (sezione 1.6 e [3], clausole 6.1.3e e 8.3);
- i documenti necessari all'esecuzione di controlli selezionati (sezione 1.6 e [3], allegato A).

(38) Gli operatori delle stazioni C-ITS devono inoltre produrre e conservare la seguente documentazione a riprova dei risultati conseguiti:

- la documentazione relativa alla formazione, alle competenze, all'esperienza e alle qualifiche ([3], clausola 7.2);

- i risultati del monitoraggio e delle misurazioni ([3], clausola 9.1);
- il programma di audit interno ([3], clausola 9.2);
- i risultati degli audit interni ([3], clausola 9.2);
- i risultati del riesame della direzione ([3], clausola 9.3);
- i risultati delle azioni correttive ([3], clausola 10.1).

2. RIFERIMENTI

Nel presente allegato si rimanda ai seguenti riferimenti:

[1] Allegato III del presente regolamento.

[2] ISO/IEC 27000 (2016): Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario

[3] ISO/IEC 27001 (2015): Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti

[4] ISO/IEC 27005 (2011): Tecnologia dell'informazione - Tecniche di sicurezza - Gestione del rischio della sicurezza delle informazioni

[5] ETSI TR 102 893 V1.2.1, Intelligent transport systems (ITS) – security; threat, vulnerability and risk analysis (TVRA)

[6] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[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

[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

[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

[10] Una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata [COM(2016) 766, 30 novembre 2016]

[11] ISO/IEC 27006 2015: Tecnologia dell'informazione - Tecniche di sicurezza - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione della sicurezza delle informazioni

[12] ISO/IEC 27007 2011: Tecnologia dell'informazione - Tecniche di sicurezza - Requisiti per l'audit dei sistemi di gestione della sicurezza delle informazioni

[13] ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS); Communications architecture

[14] ETSI TS 103 097 V1.3.1. Intelligent transport systems (ITS) security; security header and certificate formats