II

(Atti non legislativi)

REGOLAMENTI

REGOLAMENTO DI ESECUZIONE (UE) 2023/203 DELLA COMMISSIONE

del 27 ottobre 2022

che stabilisce le regole per l'applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti relativi alla gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le organizzazioni di cui ai regolamenti (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011 e (UE) 2015/340 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e per le autorità competenti di cui ai regolamenti (UE) n. 748/2012, (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011, (UE) 2015/340 e (UE) n. 139/2014 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e che modifica i regolamenti (UE) n. 1178/2011, (UE) n. 748/2012, (UE) n. 965/2012, (UE) n. 139/2014, (UE) n. 1321/2014 e (UE) 2015/340 della Commissione e i regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio ([1]), in particolare l'articolo 17, paragrafo 1, lettera b), l'articolo 27, paragrafo 1, lettera a), l'articolo 31, paragrafo 1, lettera b), l'articolo 43, paragrafo 1, lettera b), l'articolo 53, paragrafo 1, lettera a) e l'articolo 62, paragrafo 15, lettera c),

considerando quanto segue:

(1) Conformemente ai requisiti essenziali di cui all'allegato II, punto 3.1, lettera b), del regolamento (UE) 2018/1139, le organizzazioni responsabili del mantenimento dell'aeronavigabilità e le organizzazioni di manutenzione devono realizzare e mantenere un sistema di gestione per gestire i rischi in materia di sicurezza.

(2) Inoltre, conformemente ai requisiti essenziali di cui all'allegato IV, punto 3.3, lettera b), e punto 5, lettera b), del regolamento (UE) 2018/1139, le organizzazioni di addestramento dei piloti, le organizzazioni di addestramento degli equipaggi di cabina, i centri aeromedici per l'equipaggio e gli operatori di dispositivi di addestramento al volo simulato devono realizzare e mantenere un sistema di gestione per gestire i rischi in materia di sicurezza.

(3) Inoltre conformemente ai requisiti essenziali di cui all'allegato V, punto 8.1, lettera c), del regolamento (UE) 2018/1139, gli operatori aerei devono realizzare e mantenere un sistema di gestione atto a gestire i rischi in materia di sicurezza.

(4) Infine conformemente ai requisiti essenziali di cui all'allegato VIII, punto 5.1, lettera c), e punto 5.4, lettera b), del regolamento (UE) 2018/1139, i fornitori di servizi di gestione del traffico aereo e della navigazione aerea, i fornitori di servizi U-space e i fornitori unici di servizi comuni di informazione, nonché le organizzazioni di addestramento e i centri aeromedici per i controllori del traffico aereo devono realizzare e mantenere un sistema di gestione atto a gestire i rischi in materia di sicurezza.

([1]) GU L 212 del 22.8.2018, pag. 1.

(5) Tali rischi in materia di sicurezza possono derivare da varie fonti, tra cui difetti di progettazione e di manutenzione, aspetti relativi alle prestazioni umane, minacce ambientali e alla sicurezza delle informazioni. È opportuno pertanto che i sistemi di gestione realizzati dall'Agenzia dell'Unione europea per la sicurezza aerea («l'Agenzia») e dalle autorità nazionali competenti e dalle organizzazioni di cui ai precedenti considerando, tengano conto non solo dei rischi in materia di sicurezza derivanti da eventi casuali, ma anche dei rischi in materia di sicurezza derivanti da minacce alla sicurezza delle informazioni in cui le falle esistenti possono essere sfruttate da individui con l'intento di nuocere. Tali rischi per la sicurezza delle informazioni sono in costante aumento nell'ambiente dell'aviazione civile poiché gli attuali sistemi informativi stanno diventando sempre più interconnessi e sempre più bersaglio di malintenzionati.

(6) I rischi associati a tali sistemi informativi non si limitano a possibili attacchi al ciberspazio, ma comprendono anche minacce che possono influire sui processi e sulle procedure nonché sulle prestazioni umane.

(7) Un numero significativo di organizzazioni utilizza già norme internazionali, come l'ISO 27001, al fine di affrontare la questione della sicurezza delle informazioni e dei dati digitali. Tali norme potrebbero non affrontare pienamente tutte le specificità dell'aviazione civile. È pertanto opportuno stabilire requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea.

(8) È essenziale che tali requisiti riguardino tutti i settori dell'aviazione e le relative interfacce, dal momento che l'aviazione è un sistema di sistemi altamente interconnesso. Essi dovrebbero pertanto applicarsi a tutte le organizzazioni e autorità competenti di cui ai regolamenti (UE) n. 748/2012 ([2]), (UE) n. 1321/2014 ([3]), (UE) n. 965/2012 ([4]), (UE) n. 1178/2011 ([5]), (UE) 2015/340 ([6]) e (UE) n. 139/2014 ([7]) della Commissione, e al regolamento di esecuzione (UE) 2021/664 della Commissione ([8]), anche a quelle che sono già tenute a disporre di un sistema di gestione conformemente alla vigente normativa dell'Unione in materia di sicurezza aerea. Alcune organizzazioni dovrebbero tuttavia essere escluse dall'ambito di applicazione del presente regolamento al fine di garantire la debita proporzionalità ai minori rischi per la sicurezza delle informazioni che esse pongono al sistema dell'aviazione.

(9) I requisiti di cui al presente regolamento dovrebbero garantire un'attuazione coerente in tutti i settori dell'aviazione, generando nel contempo un impatto minimo sulla legislazione dell'Unione in materia di sicurezza aerea già applicabile a tali settori.

([2]) Regolamento (UE) n. 748/2012 della Commissione, del 3 agosto 2012, che stabilisce le regole di attuazione per la certificazione di aeronavigabilità e ambientale di aeromobili e relativi prodotti, parti e pertinenze, nonché per la certificazione delle imprese di progettazione e di produzione (GU L 224 del 21.8.2012, pag. 1).

([3]) Regolamento (UE) n. 1321/2014 della Commissione, del 26 novembre 2014, sul mantenimento dell'aeronavigabilità di aeromobili e di prodotti aeronautici, parti e pertinenze, nonché sull'approvazione delle organizzazioni e del personale autorizzato a tali mansioni (GU L 362 del 17.12.2014, pag. 1).

([4]) Regolamento (UE) n. 965/2012 della Commissione, del 5 ottobre 2012, che stabilisce i requisiti tecnici e le procedure amministrative per quanto riguarda le operazioni di volo ai sensi del regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio (GU L 296 del 25.10.2012, pag. 1).

([5]) Regolamento (UE) n. 1178/2011 della Commissione, del 3 novembre 2011, che stabilisce i requisiti tecnici e le procedure amministrative relativamente agli equipaggi dell'aviazione civile ai sensi del regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio (GU L 311 del 25.11.2011, pag. 1).

([6]) Regolamento (UE) 2015/340 della Commissione, del 20 febbraio 2015, che stabilisce i requisiti tecnici e le procedure amministrative concernenti licenze e certificati dei controllori del traffico aereo ai sensi del regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio, modifica il regolamento di esecuzione (UE) n. 923/2012 della Commissione e abroga il regolamento (UE) n. 805/2011 della Commissione (GU L 63 del 6.3.2015, pag. 1).

([7]) Regolamento (UE) n. 139/2014 della Commissione, del 12 febbraio 2014, che stabilisce i requisiti tecnici e le procedure amministrative relativi agli aeroporti ai sensi del regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio (GU L 44 del 14.2.2014, pag. 1).

([8]) Regolamento di esecuzione (UE) 2021/664 della Commissione, del 22 aprile 2021, relativo a un quadro normativo per lo U-space (GU L 139 del 23.4.2021, pag. 161).

(10) I requisiti di cui al presente regolamento dovrebbero lasciare impregiudicati gli obblighi in materia di sicurezza delle informazioni e cibersicurezza di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998 della Commissione ([9]) e all'articolo 14 della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([10]).

(11) I requisiti stabiliti al titolo V «Sicurezza del programma», articoli da 33 a 43, del regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio ([11]) sono considerati equivalenti ai requisiti di cui al presente regolamento, tranne per quanto riguarda il punto IS.I.OR.230 dell'allegato II del presente regolamento che dovrebbe essere rispettato.

(12) Al fine di garantire la certezza del diritto, è opportuno che l'interpretazione del termine «sicurezza delle informazioni» quale definito nel presente regolamento, che riflette il suo uso comune nell'aviazione civile a livello mondiale, sia ritenuta analoga a quella del termine «sicurezza della rete e dei sistemi informativi» quale definito all'articolo 4, punto 2, della direttiva (UE) 2016/1148. La definizione di sicurezza delle informazioni utilizzata ai fini del presente regolamento non dovrebbe essere interpretata come divergente dalla definizione di sicurezza della rete e dei sistemi informativi di cui alla direttiva (UE) 2016/1148.

(13) Al fine di evitare la duplicazione dei requisiti giuridici, qualora le organizzazioni contemplate dal presente regolamento siano già soggette a obblighi di sicurezza derivanti da atti dell'Unione di cui ai considerando 10 e 11, che sono, nei relativi effetti, equivalenti alle disposizioni del presente regolamento, la conformità a tali obblighi di sicurezza dovrebbe essere considerata conforme ai requisiti stabiliti dal presente regolamento.

(14) Le organizzazioni di cui al presente regolamento che sono già soggette agli obblighi di sicurezza derivanti dal regolamento di esecuzione (UE) 2015/1998 o dal regolamento (UE) 2021/696, o da entrambi, dovrebbero inoltre conformarsi ai requisiti di cui all'allegato II (parte IS.I.OR.230 «Sistema di segnalazione esterna della sicurezza delle informazioni») del presente regolamento, poiché nessuno dei due regolamenti contiene disposizioni relative alla segnalazione esterna degli inconvenienti per la sicurezza delle informazioni.

(15) Per completezza, i regolamenti (UE) n. 1178/2011, (UE) n. 748/2012, (UE) n. 965/2012, (UE) n. 139/2014, (UE) n. 1321/2014, (UE) 2015/340, e i regolamenti di esecuzione (UE) 2017/373 ([12]) e (UE) 2021/664 dovrebbero essere modificati al fine di introdurre i requisiti per i sistemi di gestione della sicurezza delle informazioni prescritti dal presente regolamento insieme ai sistemi di gestione ivi indicati, e stabilire i requisiti delle autorità competenti per quanto riguarda la sorveglianza delle organizzazioni che attuano i suddetti requisiti di gestione della sicurezza delle informazioni.

(16) Al fine di offrire alle organizzazioni un periodo sufficiente per garantire la conformità alle nuove norme e procedure, è opportuno che il presente regolamento si applichi tre anni dopo la sua entrata in vigore, fatta eccezione per il fornitore di servizi di navigazione aerea del Servizio europeo di copertura per la navigazione geostazionaria (EGNOS) definito nel regolamento di esecuzione (UE) 2017/373, per il quale dovrebbe diventare applicabile dal 1º gennaio 2026 a causa dell'accreditamento di sicurezza in corso del sistema e dei servizi EGNOS conformemente al regolamento (UE) 2021/696.

(17) I requisiti stabiliti nel presente regolamento si basano sul parere n. 03/2021 ([13]), emesso dall'Agenzia in conformità all'articolo 75, paragrafo 2, lettere b) e c), e all'articolo 76, paragrafo 1, del regolamento (UE) 2018/1139.

([9]) Regolamento di esecuzione (UE) 2015/1998 della Commissione, del 5 novembre 2015, che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea (GU L 299 del 14.11.2015, pag. 1).

([10]) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

([11]) Regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e che abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE (GU L 170 del 12.5.2021, pag. 69).

([12]) Regolamento di esecuzione (UE) 2017/373 della Commissione, del 1º marzo 2017, che stabilisce i requisiti comuni per i fornitori di servizi di gestione del traffico aereo e di navigazione aerea e di altre funzioni della rete di gestione del traffico aereo e per la loro sorveglianza, che abroga il regolamento (CE) n. 482/2008 e i regolamenti di esecuzione (UE) n. 1034/2011, (UE) n. 1035/2011 e (UE) 2016/1377 e che modifica il regolamento (UE) n. 677/2011 (GU L 62 dell'8.3.2017, pag. 1).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) I requisiti stabiliti nel presente regolamento sono conformi al parere del comitato per l'applicazione delle norme comuni di sicurezza nel settore dell'aviazione civile, istituito dall'articolo 127 del regolamento (UE) 2018/1139,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento stabilisce i requisiti che devono essere soddisfatti dalle organizzazioni (imprese) e dalle autorità competenti al fine di:

a) individuare e gestire i rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea che potrebbero incidere sui sistemi di tecnologia dell'informazione e della comunicazione e sui dati utilizzati per finalità relative all'aviazione civile;

b) rilevare gli eventi relativi alla sicurezza delle informazioni e individuare quelli che sono considerati inconvenienti per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea;

c) rispondere a tali inconvenienti e provvedere al ripristino.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica alle organizzazioni (imprese) seguenti:

a) le imprese di manutenzione soggette all'allegato II (parte 145), sezione A, del regolamento (UE) n. 1321/2014, a eccezione di quelle che partecipano esclusivamente alla manutenzione di aeromobili conformemente all'allegato V *ter* (parte ML) del regolamento (UE) n. 1321/2014;

b) le imprese per la gestione del mantenimento dell'aeronavigabilità (CAMO) soggette all'allegato V *quater* (parte CAMO), sezione A, del regolamento (UE) n. 1321/2014, a eccezione di quelle che partecipano esclusivamente alla gestione del mantenimento dell'aeronavigabilità degli aeromobili in conformità all'allegato V *ter* (parte ML) del regolamento (UE) n. 1321/2014;

c) gli operatori aerei soggetti all'allegato III (parte ORO) del regolamento (UE) n. 965/2012, a eccezione di quelli che partecipano esclusivamente della gestione di uno dei velivoli seguenti:

   i) aeromobili ELA 2 quali definiti all'articolo 1, paragrafo 2, lettera j), del regolamento (UE) n. 748/2012;

   ii) velivoli monomotore a elica con una configurazione operativa massima di sedili passeggeri pari o inferiore a 5, che non sono classificati come aeromobili complessi a motore, quando decollano e atterrano nello stesso aerodromo o sito operativo e operano secondo le regole del volo a vista (VFR) diurno;

   iii) elicotteri monomotore con una configurazione operativa massima di sedili passeggeri pari o inferiore a 5, che non sono classificati come aeromobili complessi a motore, quando decollano e atterrano nello stesso aerodromo o sito operativo e operano secondo le regole del VFR diurno;

d) le organizzazioni di addestramento autorizzate (ATO) soggette all'allegato VII (parte ORA) del regolamento (UE) n. 1178/2011, a eccezione di quelle che partecipano esclusivamente ad attività di addestramento per aeromobili ELA 2 quali definiti all'articolo 1, paragrafo 2, lettera j), del regolamento (UE) n. 748/2012, o che partecipano esclusivamente all'addestramento teorico;

e) i centri aeromedici per equipaggi soggetti all'allegato VII (parte ORA) del regolamento (UE) n. 1178/2011;

f) gli operatori di dispositivi di addestramento al volo simulato (FSTD) soggetti all'allegato VII (parte ORA) del regolamento (UE) n. 1178/2011, a eccezione di quelli che partecipano esclusivamente alla gestione di FSTD per aeromobili ELA 2, quali definiti all'articolo 1, paragrafo 2, lettera j), del regolamento (UE) n. 748/2012;

g) le organizzazioni di addestramento dei controllori del traffico aereo (ATCO TO) e centri aeromedici ATCO soggetti all'allegato III (parte ATCO.OR) del regolamento (UE) 2015/340;

h) le organizzazioni soggette all'allegato III (parte ATM/ANS.OR) del regolamento di esecuzione (UE) 2017/373, a eccezione dei fornitori di servizi seguenti:

i) i fornitori di servizi di navigazione aerea in possesso di un certificato limitato in conformità al punto ATM/ANS.OR.A.010 di tale allegato;

ii) i fornitori di servizi di informazione di volo che dichiarano le loro attività in conformità al punto ATM/ANS.OR.A.015 di tale allegato;

i) i fornitori di servizi U-space e fornitori unici di servizi comuni di informazione soggetti al regolamento di esecuzione (UE) 2021/664.

2. Il presente regolamento si applica alle autorità competenti, compresa l'Agenzia dell'Unione europea per la sicurezza aerea («l'Agenzia»), di cui all'articolo 6 del presente regolamento e all'articolo 5 del regolamento delegato (UE) 2022/1645 della Commissione ([14])

3. Il presente regolamento si applica altresì all'autorità competente responsabile del rilascio, proroga, modifica, sospensione o revoca delle licenze di manutenzione aeronautica in conformità all'allegato III (parte 66) del regolamento (UE) n. 1321/2014.

4. Il presente regolamento lascia impregiudicati gli obblighi in materia di sicurezza delle informazioni e cibersicurezza di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998 e all'articolo 14 della direttiva (UE) 2016/1148.

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

1) «sicurezza delle informazioni»: la tutela della riservatezza, dell'integrità, dell'autenticità e della disponibilità della rete e dei sistemi informativi;

2) «evento relativo alla sicurezza delle informazioni»: un evento individuato di un sistema, di un servizio o di uno stato di rete che indica una possibile violazione della politica di sicurezza delle informazioni, o un'avaria dei controlli di sicurezza delle informazioni, o una situazione precedentemente sconosciuta che può essere pertinente per la sicurezza delle informazioni;

3) «inconveniente»: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi, definito quale «incidente» all'articolo 4, punto 7, della direttiva (UE) 2016/1148;

4) «rischio per la sicurezza delle informazioni»: il rischio per le operazioni organizzative dell'aviazione civile, i beni, le persone fisiche e altre imprese a causa del potenziale di un evento relativo alla sicurezza delle informazioni. I rischi per la sicurezza delle informazioni sono associati alla possibilità che le minacce sfruttino le vulnerabilità di una risorsa informativa o di un gruppo di risorse informative;

([14]) Regolamento delegato (UE) 2022/1645 della Commissione del 14 luglio 2022 recante modalità di applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le imprese disciplinate dai regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione e che modifica i regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione (GU L 248 del 26.9.2022, pag. 18).

5) «minaccia»: una potenziale violazione della sicurezza delle informazioni che sussiste in presenza di un'entità, una circostanza, un'azione o un evento che potrebbe nuocere;

6) «vulnerabilità»: una falla o una debolezza in un bene o in un sistema, nelle procedure, nella progettazione, nell'attuazione o nelle misure di sicurezza delle informazioni, che potrebbe essere sfruttata e che si traduce in una violazione della politica di sicurezza delle informazioni.

Articolo 4

Requisiti per le organizzazioni (imprese) e le autorità competenti

1. Le organizzazioni (imprese) di cui all'articolo 2, paragrafo 1, rispettano i requisiti dell'allegato II (parte IS.I.OR) del presente regolamento.

2. Le autorità competenti di cui all'articolo 2, paragrafi 2 e 3, rispettano i requisiti dell'allegato I (parte IS.AR) del presente regolamento.

Articolo 5

Obblighi derivanti da altre normative dell'Unione

1. Se un'impresa di cui all'articolo 2, paragrafo 1, soddisfa gli obblighi in materia di sicurezza stabiliti conformemente all'articolo 14 della direttiva (UE) 2016/1148, equivalenti agli obblighi di cui al presente regolamento, la conformità a tali obblighi di sicurezza è considerata come conformità agli obblighi di cui al presente regolamento.

2. Se un'organizzazione (impresa) di cui all'articolo 2, paragrafo 1, è un operatore o un'entità di cui ai programmi nazionali per la sicurezza dell'aviazione civile degli Stati membri stabiliti a norma dell'articolo 10 del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio ([15]), gli obblighi in materia di cibersicurezza di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998 sono considerati equivalenti ai requisiti di cui al presente regolamento, tranne per quanto riguarda il punto IS.I.OR.230 dell'allegato II del presente regolamento che è da rispettare di per sé.

3. Nei casi in cui l'organizzazione (impresa) di cui all'articolo 2, paragrafo 1, sia il fornitore di servizi di navigazione aerea del Servizio europeo di copertura per la navigazione geostazionaria (EGNOS) di cui al regolamento (UE) 2021/696, i requisiti di cui agli articoli da 33 a 43 del titolo V di tale regolamento sono considerati equivalenti ai requisiti di cui al presente regolamento, tranne per quanto riguarda il punto IS.I.OR.230 dell'allegato II del presente regolamento che è da rispettare di per sé.

4. La Commissione, previa consultazione dell'Agenzia e del gruppo di cooperazione di cui all'articolo 11 della direttiva (UE) 2016/1148, può emanare orientamenti per la valutazione dell'equivalenza tra i requisiti di cui al presente regolamento e quelli di cui alla direttiva (UE) 2016/1148.

Articolo 6

Autorità competente

1. Fatti salvi i compiti affidati al comitato di accreditamento di sicurezza (SAB) di cui all'articolo 36 del regolamento (UE) 2021/696, l'autorità responsabile della certificazione e della supervisione della conformità al presente regolamento è:

a) per quanto riguarda le imprese di cui all'articolo 2, paragrafo 1, lettera a), l'autorità competente designata conformemente all'allegato II (parte 145) del regolamento (UE) n. 1321/2014;

b) per quanto riguarda le imprese di cui all'articolo 2, paragrafo 1, lettera b), l'autorità competente designata conformemente all'allegato V *quater* (parte CAMO) del regolamento (UE) n. 1321/2014;

([15]) Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

c) per quanto riguarda le organizzazioni di cui all'articolo 2, paragrafo 1, lettera c), l'autorità competente designata conformemente all'allegato III (parte ORO) del regolamento (UE) n. 965/2012;

d) per quanto riguarda le organizzazioni di cui all'articolo 2, paragrafo 1, lettere da d) a f), l'autorità competente designata conformemente all'allegato VII (parte ORA) del regolamento (UE) n. 1178/2011;

e) per quanto riguarda le organizzazioni di cui all'articolo 2, paragrafo 1, lettera g), l'autorità competente designata conformemente all'articolo 6, paragrafo 2, del regolamento (UE) 2015/340;

f) per quanto riguarda le organizzazioni di cui all'articolo 2, paragrafo 1, lettera h), l'autorità competente designata conformemente all'articolo 4, paragrafo 1, del regolamento di esecuzione (UE) 2017/373;

g) per quanto riguarda le organizzazioni di cui all'articolo 2, paragrafo 1, lettera i), l'autorità competente designata conformemente all'articolo 14, paragrafo 1 o, se del caso, all'articolo 14, paragrafo 2, del regolamento di esecuzione (UE) 2021/664.

2. Ai fini del presente regolamento gli Stati membri possono designare un'entità indipendente e autonoma per adempiere al ruolo e alle responsabilità assegnati alle autorità competenti di cui al paragrafo 1. In tal caso, sono stabilite misure di coordinamento tra tale entità e le autorità competenti di cui al paragrafo 1, al fine di garantire una sorveglianza efficace di tutti i requisiti che l'organizzazione deve soddisfare.

3. L'Agenzia collabora, nel pieno rispetto delle norme applicabili in materia di segretezza, protezione dei dati personali e protezione delle informazioni classificate, con l'Agenzia dell'Unione europea per il programma spaziale (EUSPA) e con il SAB di cui all'articolo 36 del regolamento (UE) 2021/696, al fine di garantire una sorveglianza efficace dei requisiti applicabili al fornitore di servizi di navigazione aerea EGNOS.

Articolo 7

Invio di informazioni pertinenti alle autorità competenti per le reti e i sistemi informativi (NIS)

Le autorità competenti a norma del presente regolamento comunicano, senza indebito ritardo, al punto di contatto unico designato a norma dell'articolo 8 della direttiva (UE) 2016/1148 qualsiasi informazione pertinente inserita nelle notifiche presentate a norma dell'allegato II, punto IS.I.OR.230, del presente regolamento e dell'allegato I, punto IS.D.OR.230, del regolamento delegato 2022/1645 dagli operatori di servizi essenziali di cui all'articolo 5 della direttiva (UE) 2016/1148.

Articolo 8

Modifica del regolamento (UE) n. 1178/2011

Gli allegati VI (parte ARA) e VII (parte ORA) del regolamento (UE) n. 1178/2011 sono modificati conformemente all'allegato III del presente regolamento.

Articolo 9

Modifica del regolamento (UE) n. 748/2012

L'allegato I (parte 21) del regolamento (UE) n. 748/2012 è modificato conformemente all'allegato IV del presente regolamento.

Articolo 10

Modifica del regolamento (UE) n. 965/2012

Gli allegati II (parte ARO) e III (parte ORO) del regolamento (UE) n. 965/2012 sono modificati conformemente all'allegato V del presente regolamento.

Articolo 11

Modifica del regolamento (UE) n. 139/2014

L'allegato II (parte ADR.OR) del regolamento (UE) n. 139/2014 è modificato conformemente all'allegato VI del presente regolamento.

Articolo 12

Modifica del regolamento (UE) n. 1321/2014

Gli allegati II (parte 145), III (parte 66) e V *quater* (parte CAMO) del regolamento (UE) n. 1321/2014 sono modificati conformemente all'allegato VII del presente regolamento.

Articolo 13

Modifica del regolamento (UE) 2015/340

Gli allegati II (parte ATCO.AR) e III (parte ATCO.OR) del regolamento (UE) 2015/340 sono modificati conformemente all'allegato VIII del presente regolamento.

Articolo 14

Modifica del regolamento di esecuzione (UE) 2017/373

Gli allegati II (parte ATM/ANS.AR) e III (parte ATM/ANS.OR) del regolamento di esecuzione (UE) 2017/373 sono modificati conformemente all'allegato IX del presente regolamento.

Articolo 15

Modifica del regolamento di esecuzione (UE) 2021/664

Il regolamento di esecuzione (UE) 2021/664 è così modificato:

1) all'articolo 15, paragrafo 1, la lettera f) è sostituita dalla seguente:

«f) attuano e mantengono un sistema di gestione della sicurezza (*security*) conformemente all'allegato III, sottoparte D, punto ATM/ANS.OR.D.010 del regolamento di esecuzione (UE) 2017/373 e un sistema di gestione della sicurezza delle informazioni in conformità all'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203.»;

2) all'articolo 18 è aggiunta la seguente lettera l):

«l) istituire, attuare e mantenere un sistema di gestione della sicurezza delle informazioni in conformità all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203.».

Articolo 16

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dal 22 febbraio 2026.

Tuttavia per quanto riguarda il caso del fornitore di servizi di navigazione aerea EGNOS soggetto al regolamento di esecuzione (UE) 2017/373, esso si applica a decorrere dal 1º gennaio 2026.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 27 ottobre 2022

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

SICUREZZA DELLE INFORMAZIONI — REQUISITI DELL'AUTORITÀ

[PARTE IS.AR]

IS.AR.100 Ambito di applicazione

IS.AR.200 Sistema di gestione della sicurezza delle informazioni (ISMS)

IS.AR.205 Valutazione dei rischi per la sicurezza delle informazioni

IS.AR.210 Trattamento dei rischi per la sicurezza delle informazioni

IS.AR.215 Inconvenienti per la sicurezza delle informazioni — rilevamento, risposta e ripristino

IS.AR.220 Appalto delle attività di gestione della sicurezza delle informazioni

IS.AR.225 Requisiti relativi al personale

IS.AR.230 Archiviazione dei documenti

IS.AR.235 Miglioramento continuo

IS.AR.100 Ambito di applicazione

La presente parte stabilisce i requisiti di gestione che le autorità competenti di cui all'articolo 2, paragrafo 2, del presente regolamento devono soddisfare.

I requisiti che tali autorità competenti devono soddisfare per lo svolgimento delle loro attività di certificazione, sorveglianza e applicazione delle norme sono contenuti nei regolamenti di cui all'articolo 2, paragrafo 1, del presente regolamento e nell'articolo 2 del regolamento delegato (UE) 2022/1645.

IS.AR.200 Sistema di gestione della sicurezza delle informazioni (ISMS)

a) Al fine di conseguire gli obiettivi di cui all'articolo 1, l'autorità competente istituisce, realizza e mantiene un sistema di gestione della sicurezza delle informazioni (ISMS) che le garantisca di:

   1) stabilire una politica in materia di sicurezza delle informazioni che definisca i principi generali dell'autorità competente per quanto riguarda il potenziale impatto dei rischi per la sicurezza delle informazioni sulla sicurezza aerea;

   2) individuare e riesaminare i rischi per la sicurezza delle informazioni conformemente al punto IS.AR.205;

   3) definire e attuare le misure di trattamento dei rischi per la sicurezza delle informazioni conformemente al punto IS.AR.210;

   4) definire e attuare, conformemente al punto IS.AR.215, le misure necessarie per rilevare gli eventi relativi alla sicurezza delle informazioni, individuare gli eventi che sono considerati inconvenienti con un potenziale impatto sulla sicurezza aerea, nonché rispondere a tali inconvenienti per la sicurezza delle informazioni e provvedere al ripristino;

   5) soddisfare i requisiti di cui al punto IS.AR.220 quando appalta una parte delle attività descritte al punto IS.AR.200 ad altre organizzazioni;

   6) soddisfare i requisiti relativi al personale di cui al punto IS.AR.225;

   7) soddisfare i requisiti per l'archiviazione dei documenti di cui al punto IS.AR.230;

   8) monitorare la conformità della propria organizzazione ai requisiti del presente regolamento e fornire un feedback sulle non conformità alla persona di cui al punto IS.AR.225, lettera a), per garantire l'efficace attuazione delle azioni correttive;

9) proteggere la riservatezza delle informazioni di cui l'autorità competente può disporre in relazione alle organizzazioni soggette alla sua sorveglianza e delle informazioni ricevute attraverso i sistemi di segnalazione esterna dell'organizzazione stabiliti conformemente al punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) del presente regolamento e al punto IS.D.OR.230 dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645;

10) notificare all'agenzia i cambiamenti che influiscono sulla capacità dell'autorità competente di svolgere i propri compiti e di adempiere alle proprie responsabilità, quali definiti nel presente regolamento;

11) definire e attuare procedure per condividere, opportunamente e in modo pratico e tempestivo, le informazioni pertinenti per assistere altre autorità e organismi competenti, nonché le organizzazioni soggette al presente regolamento, nel condurre efficaci valutazioni del rischio per la sicurezza in relazione alle proprie attività.

b) Al fine di soddisfare in modo continuativo i requisiti di cui all'articolo 1, l'autorità competente attua un processo di miglioramento continuo conformemente al punto IS.AR.235.

c) L'autorità competente documenta tutti i processi, le procedure, i ruoli e le responsabilità principali necessari per conformarsi al punto IS.AR.200, lettera a), e per definire un processo di modifica di tale documentazione.

d) I processi, le procedure, i ruoli e le responsabilità stabiliti dall'autorità competente per conformarsi al punto IS.AR.200, lettera a), corrispondono alla natura e alla complessità delle sue attività, sulla base di una valutazione dei rischi per la sicurezza delle informazioni inerenti a tali attività e possono essere integrati in altri sistemi di gestione esistenti già attuati dall'autorità competente.

IS.AR.205 Valutazione dei rischi per la sicurezza delle informazioni

a) L'autorità competente individua tutti gli elementi della propria organizzazione che potrebbero essere esposti a rischi per la sicurezza delle informazioni. Tali elementi includono:

1) le attività, le strutture e le risorse dell'autorità competente, nonché i servizi che essa gestisce, fornisce, riceve o mantiene;

2) le apparecchiature, i sistemi, i dati e le informazioni che contribuiscono al funzionamento degli elementi di cui al punto 1).

b) L'autorità competente individua le interfacce che la propria organizzazione ha con altre organizzazioni che potrebbero comportare l'esposizione reciproca a rischi per la sicurezza delle informazioni.

c) Per quanto riguarda gli elementi e le interfacce di cui alle lettere a) e b), l'autorità competente individua i rischi per la sicurezza delle informazioni che possono avere un potenziale impatto sulla sicurezza aerea.

Per ogni rischio individuato l'autorità:

1) assegna un livello di rischio secondo una classificazione predefinita stabilita dall'autorità competente stessa;

2) associa ciascun rischio e il suo livello all'elemento o all'interfaccia corrispondenti individuati conformemente alle lettere a) e b).

La classificazione predefinita di cui al punto 1) tiene conto del potenziale di insorgenza dello scenario di minaccia e della gravità delle sue conseguenze per la sicurezza. Mediante tale classificazione, e considerando se l'autorità competente disponga di un processo operativo di gestione dei rischi strutturato e ripetibile, l'autorità competente medesima è in grado di stabilire se il rischio sia accettabile o debba essere trattato conformemente al punto IS.AR.210.

Al fine di agevolare la comparabilità reciproca delle valutazioni dei rischi, l'assegnazione del livello di rischio di cui al punto 1) tiene conto delle informazioni pertinenti acquisite in coordinamento con le organizzazioni di cui alla lettera b).

d) L'autorità competente riesamina e aggiorna la valutazione dei rischi effettuata conformemente alle lettere a), b) e c) in uno dei casi seguenti:

1) in caso di una modifica degli elementi soggetti a rischi per la sicurezza delle informazioni;

2) in caso di una modifica delle interfacce tra l'autorità competente e le altre organizzazioni, oppure dei rischi comunicati da queste ultime;

3) in caso di una modifica delle informazioni o delle conoscenze utilizzate per l'individuazione, l'analisi e la classificazione dei rischi;

4) in caso di insegnamenti tratti dall'analisi degli inconvenienti per la sicurezza delle informazioni.

IS.AR.210 Trattamento dei rischi per la sicurezza delle informazioni

a) L'autorità competente elabora misure per affrontare i rischi inaccettabili individuati conformemente al punto IS.AR.205, le attua tempestivamente e ne verifica l'efficacia nel tempo. Tali misure consentono all'autorità competente di:

1) controllare le circostanze che contribuiscono all'effettivo verificarsi dello scenario di minaccia;

2) ridurre le conseguenze per la sicurezza aerea associate al verificarsi dello scenario di minaccia;

3) evitare i rischi.

Tali misure non introducono nuovi potenziali rischi inaccettabili per la sicurezza aerea.

b) La persona di cui al punto IS.AR.225, lettera a) e gli altri membri del personale interessati dell'autorità competente sono informati dell'esito della valutazione dei rischi effettuata conformemente al punto IS.AR.205, dei corrispondenti scenari di minaccia e delle misure da attuare.

L'autorità competente informa inoltre le organizzazioni con le quali ha un'interfaccia conformemente al punto IS.AR.205, lettera b), di qualsiasi rischio condiviso tra la l'autorità competente e l'organizzazione.

IS.AR.215 Inconvenienti per la sicurezza delle informazioni — rilevamento, risposta e ripristino

a) Sulla base dell'esito della valutazione dei rischi effettuata conformemente al punto IS.AR.205 e dell'esito del trattamento dei rischi effettuato conformemente al punto IS.AR.210, l'autorità competente attua misure per rilevare gli eventi che indicano il potenziale verificarsi di rischi inaccettabili e che possono avere un potenziale impatto sulla sicurezza aerea. Tali misure di rilevamento consentono all'autorità competente di:

1) individuare le deviazioni dai livelli di base predeterminati delle prestazioni funzionali;

2) attivare avvisi per avviare misure di risposta adeguate, in caso di deviazione.

b) L'autorità competente attua misure per rispondere a qualsiasi evento individuato in conformità alla lettera a), che può trasformarsi o si è trasformato in un inconveniente nel settore della sicurezza delle informazioni. Tali misure di risposta consentono all'autorità competente di:

1) avviare la reazione della propria organizzazione agli avvisi di cui alla lettera a), punto 2), attivando risorse e procedure predefinite;

2) contenere la diffusione di un attacco ed evitare il completo verificarsi di uno scenario di minaccia;

3) controllare la modalità di guasto degli elementi interessati definiti al punto IS.AR.205, lettera a).

c) L'autorità competente attua misure volte al ripristino dopo inconvenienti per la sicurezza delle informazioni, comprese, se necessario, misure di emergenza. Tali misure di ripristino consentono all'autorità competente di:

1) eliminare la condizione che ha causato l'inconveniente o limitarla a un livello tollerabile;

2) ripristinare uno stato di sicurezza degli elementi interessati definiti al punto IS.AR.205, lettera a), entro un tempo di recupero precedentemente definito dalla propria organizzazione.

IS.AR.220 Appalto delle attività di gestione della sicurezza delle informazioni

L'autorità competente garantisce che, nell'appaltare una parte delle attività di cui al punto IS.AR.200 ad altre organizzazioni, le attività oggetto dell'appalto siano conformi ai requisiti del presente regolamento e che l'impresa appaltatrice lavori sotto la sua sorveglianza. L'autorità competente garantisce che i rischi associati alle attività oggetto dell'appalto siano adeguatamente gestiti.

IS.AR.225 Requisiti relativi al personale

L'autorità competente deve:

a) disporre di una persona che abbia l'autorità di creare e mantenere le strutture organizzative, le politiche, i processi e le procedure necessari per l'attuazione del presente regolamento.

Tale persona deve:

1) avere l'autorità di accedere pienamente alle risorse necessarie all'autorità competente per svolgere tutti i compiti richiesti dal presente regolamento;

2) avere la delega di potere necessaria per svolgere i compiti assegnati;

b) disporre di un processo atto a garantire la presenza di personale sufficiente per svolgere le attività contemplate dal presente allegato;

c) disporre di un processo atto a garantire che il personale di cui alla lettera b) abbia le competenze necessarie per svolgere i propri compiti;

d) disporre di un processo atto a garantire che il personale riconosca le responsabilità associate ai ruoli e ai compiti assegnati;

e) garantire che l'identità e l'affidabilità del personale che ha accesso ai sistemi informativi e ai dati soggetti ai requisiti del presente regolamento siano adeguatamente accertate.

IS.AR.230 Archiviazione dei documenti

a) L'autorità competente archivia i documenti relativi alle proprie attività di gestione della sicurezza delle informazioni.

1) L'autorità competente garantisce che siano archiviati e tracciabili i documenti seguenti:

i) gli appalti delle attività di cui al punto IS.AR.200, lettera a), punto 5);

ii) i registri dei processi principali di cui al punto IS.AR.200, lettera d);

iii) i registri dei rischi individuati nella valutazione dei rischi di cui al punto IS.AR.205 e le relative misure di trattamento degli stessi di cui al punto IS.AR.210;

iv) i registri riguardanti gli eventi relativi alla sicurezza delle informazioni che potrebbe essere necessario rivalutare per individuare inconvenienti o vulnerabilità relativi alla sicurezza delle informazioni non rilevati.

2) I registri di cui al punto 1.i), sono conservati almeno fino a cinque anni dalla modifica o risoluzione dell'appalto.

3) I registri di cui ai punti 1.ii) e 1.iii) sono conservati almeno per un periodo di cinque anni.

4) I registri di cui al punto 1.iv), sono conservati fino a quando tali eventi relativi alla sicurezza delle informazioni non siano stati rivalutati secondo una periodicità definita in una procedura stabilita dall'autorità competente.

b) L'autorità competente conserva i dati relativi alle qualifiche e all'esperienza del proprio personale che partecipa alle attività di gestione della sicurezza delle informazioni.

1) I dati relativi alle qualifiche e all'esperienza del personale sono conservati per tutto il tempo in cui la persona lavora per l'autorità competente e per almeno tre anni dalla cessazione del rapporto di lavoro.

2) Su richiesta, i membri del personale hanno accesso ai loro dati individuali. Inoltre, sempre dietro richiesta, l'autorità competente fornisce loro una copia dei rispettivi dati individuali al momento della cessazione del rapporto di lavoro.

c) Il formato dei dati è specificato nelle procedure dell'autorità competente.

d) I dati sono conservati in modo da garantire la protezione da danni, alterazioni e furti, identificando le informazioni, se necessario, in base al loro livello di classificazione di sicurezza. L'autorità competente garantisce che i dati siano conservati utilizzando strumenti che garantiscano l'integrità, l'autenticità e l'accesso autorizzato.

IS.AR.235 Miglioramento continuo

a) L'autorità competente valuta, utilizzando adeguati indicatori di prestazione, l'efficacia e la maturità dell'ISMS. Tale valutazione è effettuata sulla base di un calendario predefinito dall'autorità competente o a seguito di un inconveniente nel settore della sicurezza delle informazioni.

b) Se si riscontrano carenze a seguito della valutazione effettuata conformemente alla lettera a), l'autorità competente adotta le misure di miglioramento necessarie per garantire che l'ISMS continui a rispettare i requisiti applicabili e mantenga i rischi per la sicurezza delle informazioni a un livello accettabile. L'autorità competente riesamina inoltre gli elementi dell'ISMS interessati dalle misure adottate.

ALLEGATO II

SICUREZZA DELLE INFORMAZIONI — REQUISITI PER LE ORGANIZZAZIONI

[PARTE IS.I.OR]

IS.I.OR.100 Ambito di applicazione

IS.I.OR.200 Sistema di gestione della sicurezza delle informazioni (ISMS)

IS.I.OR.205 Valutazione dei rischi per la sicurezza delle informazioni

IS.I.OR.210 Trattamento dei rischi per la sicurezza delle informazioni

IS.I.OR.215 Sistema di segnalazione interna della sicurezza delle informazioni

IS.I.OR.220 Inconvenienti per la sicurezza delle informazioni — rilevamento, risposta e ripristino

IS.I.OR.225 Risposte alle non conformità notificate dall'autorità competente

IS.I.OR.230 Sistema di segnalazione esterna della sicurezza delle informazioni

IS.I.OR.235 Appalto delle attività di gestione della sicurezza delle informazioni

IS.I.OR.240 Requisiti relativi al personale

IS.I.OR.245 Archiviazione dei documenti

IS.I.OR.250 Manuale di gestione della sicurezza delle informazioni (ISMM)

IS.I.OR.255 Modifiche del sistema di gestione della sicurezza delle informazioni

IS.I.OR.260 Miglioramento continuo

IS.I.OR.100 Ambito di applicazione

La presente parte stabilisce i requisiti che le organizzazioni di cui all'articolo 2, paragrafo 1, del presente regolamento devono soddisfare.

IS.I.OR.200 Sistema di gestione della sicurezza delle informazioni (ISMS)

a) Al fine di conseguire gli obiettivi di cui all'articolo 1, l'organizzazione istituisce, attua e mantiene un sistema di gestione della sicurezza delle informazioni (ISMS) che le garantisca di:

   1) stabilire una politica in materia di sicurezza delle informazioni che definisca i principi generali dell'organizzazione per quanto riguarda il potenziale impatto dei rischi per la sicurezza delle informazioni sulla sicurezza aerea;

   2) individuare e riesaminare i rischi per la sicurezza delle informazioni conformemente al punto IS.I.OR.205;

   3) definire e attuare le misure di trattamento dei rischi per la sicurezza delle informazioni conformemente al punto IS.I.OR.210;

   4) attuare un sistema di segnalazione interna per la sicurezza delle informazioni conformemente al punto IS.I.OR.215;

   5) definire e attuare, conformemente al punto IS.I.OR.220, le misure necessarie per rilevare gli eventi relativi alla sicurezza delle informazioni, individuare gli eventi che sono considerati inconvenienti con un potenziale impatto sulla sicurezza aerea, salvo quanto consentito dal punto IS.I.OR.205, lettera e), nonché rispondere a tali inconvenienti e provvedere al ripristino;

6) attuare le misure indicate dall'autorità competente come reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea;

7) adottare le misure appropriate, conformemente al punto IS.I.OR.225, per rispondere alle non conformità notificate dall'autorità competente;

8) attuare un sistema di segnalazione esterna conformemente al punto IS.I.OR.230 al fine di consentire all'autorità competente di adottare le misure appropriate;

9) soddisfare i requisiti di cui al punto IS.I.OR.235 quando appalta una parte delle attività di cui al punto IS.I.OR.200 ad altre organizzazioni;

10) soddisfare i requisiti relativi al personale di cui al punto IS.I.OR.240;

11) soddisfare i requisiti per l'archiviazione dei documenti di cui al punto IS.I.OR.245;

12) controllare la conformità dell'organizzazione ai requisiti del presente regolamento e fornire un riscontro sulle non conformità al dirigente responsabile, al fine di garantire un'efficace attuazione delle azioni correttive;

13) proteggere, fatti salvi i requisiti applicabili in materia di segnalazione degli inconvenienti, la riservatezza di tutte le informazioni che l'organizzazione potrebbe aver ricevuto da altre organizzazioni, a seconda del relativo livello di sensibilità.

b) Al fine di soddisfare in modo continuativo i requisiti di cui all'articolo 1, l'organizzazione attua un processo di miglioramento continuo conformemente al punto IS.I.OR.260.

c) L'organizzazione documenta, conformemente al punto IS.I.OR.250, tutti i processi, le procedure, i ruoli e le responsabilità principali necessari per conformarsi al punto IS.I.OR.200, lettera a), e definisce un processo di modifica di tale documentazione. Le modifiche a tali processi, procedure, ruoli e responsabilità sono gestite conformemente al punto IS.I.OR.255.

d) I processi, le procedure, i ruoli e le responsabilità stabiliti dall'organizzazione per conformarsi al punto IS.I.OR.200, lettera a), corrispondono alla natura e alla complessità delle sue attività, sulla base di una valutazione dei rischi per la sicurezza delle informazioni inerenti a tali attività e possono essere integrati in altri sistemi di gestione esistenti già attuati dall'organizzazione.

e) Fatto salvo l'obbligo di rispettare gli obblighi di segnalazione di cui al regolamento (UE) n. 376/2014 e i requisiti di cui al punto IS.I.OR.200, lettera a), punto 13), l'organizzazione può essere autorizzata dall'autorità competente a non attuare i requisiti di cui alle lettere da a) a d) e i relativi requisiti contenuti ai punti da IS.I.OR.205 a IS.I.OR.260, se dimostra, in modo giudicato soddisfacente da detta autorità, che le sue attività, strutture e risorse, nonché i servizi che gestisce, fornisce, riceve e mantiene, non comportano rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea né per se stessa né per altre imprese. L'approvazione si basa su una valutazione documentata dei rischi per la sicurezza delle informazioni effettuata dall'organizzazione o da un terzo conformemente al punto IS.I.OR.205 e riesaminata e approvata dalla sua autorità competente.

Il mantenimento della validità di tale approvazione sarà riesaminato dall'autorità competente a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta le modifiche siano attuate nell'ambito del lavoro dell'organizzazione.

IS.I.OR.205 Valutazione dei rischi per la sicurezza delle informazioni

a) L'organizzazione individua tutti i suoi elementi che potrebbero essere esposti a rischi per la sicurezza delle informazioni. Ciò comprende:

1) le attività, le strutture e le risorse dell'organizzazione, nonché i servizi che essa gestisce, fornisce, riceve o mantiene;

2) le apparecchiature, i sistemi, i dati e le informazioni che contribuiscono al funzionamento degli elementi elencati al punto 1).

b) L'organizzazione individua le interfacce che ha con altre organizzazioni e che potrebbero comportare l'esposizione reciproca a rischi per la sicurezza delle informazioni.

c) Per quanto riguarda gli elementi e le interfacce di cui alle lettere a) e b), l'organizzazione individua i rischi per la sicurezza delle informazioni che possono avere un potenziale impatto sulla sicurezza aerea. Per ogni rischio individuato l'organizzazione:

1) assegna un livello di rischio secondo una classificazione predefinita stabilita dall'organizzazione stessa;

2) associa ciascun rischio e il suo livello all'elemento o all'interfaccia corrispondenti individuati conformemente alle lettere a) e b).

La classificazione predefinita di cui al punto 1) tiene conto del potenziale di insorgenza dello scenario di minaccia e della gravità delle sue conseguenze per la sicurezza. Sulla base di tale classificazione e tenendo conto del fatto che l'organizzazione dispone di un processo operativo di gestione dei rischi strutturato e ripetibile, l'organizzazione è in grado di stabilire se il rischio è accettabile o deve essere trattato conformemente al punto IS.I.OR.210.

Al fine di agevolare la comparabilità reciproca delle valutazioni dei rischi, l'assegnazione del livello di rischio a norma del punto 1) tiene conto delle informazioni pertinenti acquisite in coordinamento con le organizzazioni di cui alla lettera b).

d) L'organizzazione riesamina e aggiorna la valutazione dei rischi effettuata conformemente alle lettere a), b) e, se del caso, c) o e) in una delle situazioni seguenti:

1) in caso di una modifica degli elementi soggetti a rischi per la sicurezza delle informazioni;

2) in caso di una modifica delle interfacce tra l'organizzazione e le altre organizzazioni, oppure dei rischi comunicati da queste ultime;

3) in caso di una modifica delle informazioni o delle conoscenze utilizzate per l'individuazione, l'analisi e la classificazione dei rischi;

4) in caso di insegnamenti tratti dall'analisi degli inconvenienti per la sicurezza delle informazioni.

e) In deroga alla lettera c), le organizzazioni tenute a rispettare la sottoparte C dell'allegato III (parte ATM/ANS.OR) del regolamento di esecuzione (UE) 2017/373 sostituiranno l'analisi dell'impatto sulla sicurezza aerea con un'analisi dell'impatto sui loro servizi come da valutazione del sostegno alla sicurezza richiesta dal punto ATM/ANS.OR.C.005. Tale valutazione del sostegno alla sicurezza sarà resa disponibile ai fornitori di servizi di traffico aereo ai quali forniscono servizi e tali fornitori di servizi di traffico aereo saranno responsabili della valutazione dell'impatto sulla sicurezza aerea.

IS.I.OR.210 Trattamento dei rischi per la sicurezza delle informazioni

a) L'organizzazione elabora misure per affrontare i rischi inaccettabili individuati conformemente al punto IS.I.OR.205, le attua tempestivamente e ne verifica l'efficacia nel tempo. Tali misure consentono all'organizzazione di:

1) controllare le circostanze che contribuiscono all'effettivo verificarsi dello scenario di minaccia;

2) ridurre le conseguenze sulla sicurezza aerea associate al verificarsi dello scenario di minaccia;

3) evitare i rischi.

Tali misure non introducono nuovi potenziali rischi inaccettabili per la sicurezza aerea.

b) La persona di cui al punto IS.I.OR.240, lettere a) e b), e gli altri membri del personale interessati dell'organizzazione sono informati dell'esito della valutazione dei rischi effettuata conformemente al punto IS.I.OR.205, dei corrispondenti scenari di minaccia e delle misure da attuare.

L'organizzazione informa inoltre le organizzazioni con le quali ha un'interfaccia conformemente al punto IS.I.OR.205, lettera b), di qualsiasi rischio condiviso tra le due organizzazioni.

IS.I.OR.215 Sistema di segnalazione interna della sicurezza delle informazioni

a) L'organizzazione istituisce un sistema di segnalazione interna per consentire la raccolta e la valutazione degli eventi relativi alla sicurezza delle informazioni, compresi quelli da segnalare ai sensi del punto IS.I.OR.230.

b) Tale sistema e il processo di cui al punto IS.I.OR.220 consentono all'organizzazione di:

1) individuare quali degli eventi segnalati a norma della lettera a) sono considerati inconvenienti o vulnerabilità relativi alla sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea;

2) individuare le cause e i fattori che contribuiscono agli inconvenienti e alle vulnerabilità relativi alla sicurezza delle informazioni individuati conformemente al punto 1) e affrontarli nell'ambito del processo di gestione dei rischi per la sicurezza delle informazioni conformemente ai punti IS.I.OR.205 e IS.I.OR.220;

3) garantire una valutazione di tutte le informazioni note e pertinenti in merito agli inconvenienti e alle vulnerabilità relativi alla sicurezza delle informazioni individuati conformemente al punto 1);

4) garantire l'attuazione di un metodo per distribuire internamente le informazioni, se necessario.

c) Qualsiasi impresa appaltatrice che possa esporre l'organizzazione a rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea è tenuta a segnalare alla stessa gli eventi relativi alla sicurezza delle informazioni. Tali segnalazioni sono presentate secondo le procedure stabilite negli accordi contrattuali specifici e sono valutate conformemente alla lettera b).

d) L'organizzazione coopera alle indagini con qualsiasi altra organizzazione che fornisca un contributo significativo alla sicurezza delle informazioni delle proprie attività.

e) L'organizzazione può integrare tale sistema di segnalazione con altri sistemi di segnalazione già attuati.

IS.I.OR.220 Inconvenienti per la sicurezza delle informazioni — rilevamento, risposta e ripristino

a) Sulla base dell'esito della valutazione dei rischi effettuata conformemente al punto IS.I.OR.205 e dell'esito del trattamento dei rischi effettuato conformemente al punto IS.I.OR.210, l'organizzazione attua misure per rilevare gli inconvenienti e le vulnerabilità che indicano il potenziale verificarsi di rischi inaccettabili e che possono avere un potenziale impatto sulla sicurezza aerea. Tali misure di rilevamento consentono all'organizzazione di:

1) individuare le deviazioni dai livelli di base predeterminati delle prestazioni funzionali;

2) attivare avvisi per avviare misure di risposta adeguate, in caso di deviazione.

b) L'organizzazione attua misure per rispondere a qualsiasi evento individuato in conformità alla lettera a), che può trasformarsi o si è trasformato in un inconveniente nel settore della sicurezza delle informazioni. Tali misure di risposta consentono all'organizzazione di:

1) avviare la reazione agli avvisi di cui alla lettera a), punto 2), attivando risorse e procedure predefinite;

2) contenere la diffusione di un attacco ed evitare il completo verificarsi di uno scenario di minaccia;

3) controllare la modalità di guasto degli elementi interessati definiti al punto IS.I.OR.205, lettera a).

c) L'organizzazione attua misure volte al ripristino dopo inconvenienti per la sicurezza delle informazioni, comprese, se necessario, misure di emergenza. Tali misure di ripristino consentono all'organizzazione di:

1) eliminare la condizione che ha causato l'inconveniente o limitarla a un livello tollerabile;

2) raggiungere uno stato di sicurezza degli elementi interessati definiti al punto IS.I.OR.205, lettera a), entro un tempo di ripristino precedentemente definito dall'organizzazione.

IS.I.OR.225 Risposte alle non conformità notificate dall'autorità competente

a) Dopo aver ricevuto la notifica delle non conformità presentate dall'autorità competente, l'organizzazione:

1) individua la causa o le cause alla base delle non conformità e i fattori che vi contribuiscono;

2) definisce un piano di azioni correttive;

3) dimostra la correzione della non conformità in modo giudicato soddisfacente dall'autorità competente.

b) Le azioni di cui alla lettera a) sono eseguite entro il termine concordato con l'autorità competente.

IS.I.OR.230 Sistema di segnalazione esterna della sicurezza delle informazioni

a) L'organizzazione attua un sistema di segnalazione della sicurezza delle informazioni conforme agli obblighi di cui al regolamento (UE) n. 376/2014 e ai suoi atti delegati e di esecuzione se tale regolamento è applicabile all'organizzazione.

b) Fatti salvi gli obblighi del regolamento (UE) n. 376/2014, l'organizzazione garantisce che qualsiasi inconveniente o vulnerabilità riguardante la sicurezza delle informazioni che possa rappresentare un rischio significativo per la sicurezza aerea sia segnalato o segnalata alla relativa autorità competente. Inoltre:

1) se tale inconveniente o vulnerabilità riguarda un aeromobile o un sistema o componente associato, l'organizzazione segnala il fatto anche al titolare dell'approvazione del progetto;

2) se tale inconveniente o vulnerabilità riguarda un sistema o un componente utilizzato dall'organizzazione, quest'ultima lo segnala all'organizzazione responsabile della progettazione del sistema o del componente.

c) L'organizzazione comunica le condizioni di cui alla lettera b) come segue:

1) una notifica è presentata all'autorità competente e, se del caso, al titolare dell'approvazione del progetto o all'organizzazione responsabile della progettazione del sistema o del componente, non appena l'organizzazione viene a conoscenza della condizione;

2) una segnalazione è presentata all'autorità competente e, se del caso, al titolare dell'approvazione del progetto o all'organizzazione responsabile della progettazione del sistema o del componente il prima possibile, ma non oltre 72 ore dal momento in cui l'organizzazione è venuta a conoscenza della condizione, a meno che circostanze eccezionali non lo impediscano.

La segnalazione è redatta nella forma definita dall'autorità competente e contiene tutte le informazioni pertinenti relative alla condizione nota all'organizzazione;

3) una segnalazione di follow-up è presentata all'autorità competente e, se del caso, al titolare dell'approvazione del progetto o all'organizzazione responsabile della progettazione del sistema o del componente, fornendo i dettagli delle azioni che l'organizzazione ha intrapreso o intende intraprendere per il ripristino dopo l'inconveniente, e delle azioni che intende intraprendere per evitare inconvenienti analoghi per la sicurezza delle informazioni in futuro.

La segnalazione di follow-up è presentata non appena tali azioni sono state individuate ed è redatta nella forma definita dall'autorità competente.

IS.I.OR.235 Appalto delle attività di gestione della sicurezza delle informazioni

a) L'organizzazione garantisce che, nell'appaltare una parte delle attività di cui al punto IS.I.OR.200 ad altre organizzazioni, le attività oggetto dell'appalto siano conformi ai requisiti del presente regolamento e l'impresa appaltatrice lavori sotto la sua sorveglianza. L'organizzazione garantisce che i rischi associati alle attività oggetto dell'appalto siano adeguatamente gestiti.

b) L'organizzazione garantisce che l'autorità competente abbia modo di accedere, su richiesta, all'organizzazione appaltatrice per stabilire la costante conformità ai requisiti applicabili di cui al presente regolamento.

IS.I.OR.240 Requisiti relativi al personale

a) Il dirigente responsabile dell'organizzazione designato conformemente ai regolamenti (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011, (UE) 2015/340, e al regolamento di esecuzione (UE) 2017/373 o al regolamento di esecuzione (UE) 2021/664, a seconda dei casi di cui all'articolo 2, paragrafo 1, del presente regolamento, ha l'autorità giuridica necessaria per assicurare che tutte le attività richieste dal presente regolamento possano essere finanziate ed eseguite. Tale persona:

1) garantisce la disponibilità di tutte le risorse necessarie per conformarsi ai requisiti del presente regolamento;

2) stabilisce e promuove la politica in materia di sicurezza delle informazioni di cui al punto IS.I.OR.200, lettera a), punto 1);

3) dimostra una comprensione di base del presente regolamento.

b) Il dirigente responsabile nomina una persona o un gruppo di persone che garantisca la conformità dell'organizzazione ai requisiti del presente regolamento, e definisce la portata della loro autorità. Tale persona o gruppo di persone riferisce direttamente al dirigente responsabile e dispone delle conoscenze, della preparazione e dell'esperienza adeguate per assolvere le proprie responsabilità. Nelle procedure è stabilito chi farà le veci di una determinata persona in caso di prolungata assenza della stessa.

c) Il dirigente responsabile nomina una persona o un gruppo di persone responsabile della gestione della funzione di monitoraggio della conformità di cui al punto IS.I.OR.200, lettera a), punto 12).

d) Se l'organizzazione condivide strutture organizzative, politiche, processi e procedure relativi alla sicurezza delle informazioni con altre organizzazioni o con settori della propria organizzazione che non fanno parte dell'approvazione o della dichiarazione, il dirigente responsabile può delegare le proprie attività a una persona responsabile comune.

In tal caso, sono stabilite misure di coordinamento tra il dirigente responsabile dell'organizzazione e la persona responsabile comune per garantire un'adeguata integrazione della gestione della sicurezza delle informazioni all'interno dell'organizzazione.

e) Il dirigente responsabile o la persona responsabile comune di cui alla lettera d) ha l'autorità giuridica per creare e mantenere le strutture organizzative, le politiche, le procedure e i processi necessari all'attuazione del punto IS.I.OR.200.

f) L'organizzazione dispone di un processo atto a garantire la presenza di personale sufficiente per svolgere le attività contemplate dal presente allegato.

g) L'organizzazione dispone di un processo atto a garantire che il personale di cui alla lettera f) abbia le competenze necessarie per svolgere i propri compiti.

h) L'organizzazione dispone di un processo atto a garantire che il personale riconosca le responsabilità associate ai ruoli e ai compiti assegnati.

i) L'organizzazione garantisce che l'identità e l'affidabilità del personale che ha accesso ai sistemi informativi e ai dati soggetti ai requisiti del presente regolamento siano adeguatamente accertate.

IS.I.OR.245 Archiviazione dei documenti

a) *L'organizzazione archivia i documenti delle proprie attività di gestione della sicurezza delle informazioni.*

1) L'organizzazione garantisce che siano archiviati e tracciabili i documenti seguenti:

i) qualsiasi approvazione ricevuta e qualsiasi relativa valutazione dei rischi per la sicurezza delle informazioni conformemente al punto IS.I.OR.200, lettera e);

ii) gli appalti delle attività di cui al punto IS.I.OR.200, lettera a), punto 9);

iii) i registri dei processi principali di cui al punto IS.I.OR.200, lettera d);

iv) i registri dei rischi individuati nella valutazione dei rischi di cui al punto IS.I.OR.205 e le relative misure di trattamento degli stessi di cui al punto IS.I.OR.210;

v) i registri degli inconvenienti e delle vulnerabilità relativi alla sicurezza delle informazioni comunicati conformemente ai sistemi di segnalazione di cui ai punti IS.I.OR.215 e IS.I.OR.230;

vi) i registri di quegli eventi relativi alla sicurezza delle informazioni che potrebbero dover essere rivalutati per individuare inconvenienti o vulnerabilità relativi alla sicurezza delle informazioni non rilevati.

2) I registri di cui al punto 1.i), sono conservati almeno fino a cinque anni dal termine della validità dell'approvazione.

3) I registri di cui al punto 1.ii), sono conservati almeno fino a cinque anni dalla modifica o risoluzione dell'appalto.

4) I registri di cui ai punti 1.iii), 1.iv) e 1.v), sono conservati almeno per un periodo di cinque anni.

5) I registri di cui al punto 1.vi), sono conservati fino a quando tali eventi relativi alla sicurezza delle informazioni non siano stati rivalutati secondo una periodicità definita in una procedura stabilita dall'organizzazione.

b) *L'organizzazione conserva i registri delle qualifiche e dell'esperienza del proprio personale che partecipa alle attività di gestione della sicurezza delle informazioni.*

1) I registri delle qualifiche e dell'esperienza del personale sono conservati per tutto il tempo in cui la persona lavora per l'organizzazione e per almeno tre anni dalla cessazione del rapporto di lavoro con la stessa.

2) Su richiesta, i membri del personale hanno accesso ai loro dati individuali. Su richiesta, l'organizzazione fornisce loro inoltre una copia dei rispettivi registri individuali al momento della cessazione del rapporto di lavoro con la stessa.

c) Il formato dei registri è specificato nelle procedure dell'organizzazione.

d) I registri sono conservati in modo da garantire la protezione da danni, alterazioni e furti, identificando le informazioni, se necessario, in base al loro livello di classificazione di sicurezza. L'organizzazione garantisce che i registri siano conservati utilizzando strumenti che garantiscano l'integrità, l'autenticità e l'accesso autorizzato.

IS.I.OR.250 Manuale di gestione della sicurezza delle informazioni (ISMM)

a) L'organizzazione mette a disposizione dell'autorità competente un manuale di gestione della sicurezza delle informazioni (ISMM) e, se del caso, manuali e procedure di riferimento associati e pertinenti, contenenti:

1) una dichiarazione firmata dal dirigente responsabile, attestante che l'organizzazione opera in qualsiasi momento conformemente al presente allegato a all'ISMM. Qualora il dirigente responsabile non sia l'amministratore delegato (CEO) dell'organizzazione, quest'ultimo controfirma la dichiarazione;

2) il titolo (o i titoli), il nome (o i nomi), i compiti, le responsabilità e le autorità della persona o delle persone definite al punto IS.I.OR.240, lettere b) e c);

3) il titolo, il nome, i compiti, le responsabilità e l'autorità della persona responsabile comune definita al punto IS.I.OR.240, lettera d), se del caso;

4) la politica in materia di sicurezza delle informazioni dell'organizzazione di cui al punto IS.I.OR.200, lettera a), punto 1);

5) una descrizione generale del numero e delle categorie del personale e del sistema in atto per pianificare la disponibilità del personale, come richiesto al punto IS.I.OR.240;

6) il titolo (o i titoli), il nome (o i nomi), i compiti, le responsabilità e le autorità delle persone di riferimento responsabili dell'attuazione del punto IS.I.OR.200, tra cui la persona o le persone responsabili della funzione di monitoraggio della conformità di cui al punto IS.I.OR.200, lettera a), punto 12);

7) un organigramma che mostri le catene di responsabilità associate riguardanti le persone di cui ai punti 2) e 6);

8) la descrizione del sistema di segnalazione interna di cui al punto IS.I.OR.215;

9) le procedure che specificano in che modo l'organizzazione garantisce la conformità alla presente parte, in particolare:

i) la documentazione di cui al punto IS.I.OR.200, lettera c);

ii) le procedure che definiscono il modo in cui l'organizzazione controlla le attività appaltate di cui al punto IS. I.OR.200, lettera a), punto 9);

iii) la procedura di modifica dell'ISMM di cui alla lettera c);

10) i dettagli dei metodi alternativi di rispondenza attualmente approvati.

b) Il rilascio iniziale dell'ISMM è approvato e l'autorità competente ne conserva una copia. L'ISMM è modificato in base alle necessità per riflettere sempre una descrizione aggiornata dell'ISMS dell'organizzazione. Una copia delle eventuali modifiche dell'ISMM è fornita all'autorità competente.

c) Le modifiche all'ISMM sono gestite secondo una procedura stabilita dall'organizzazione. Le modifiche non incluse nell'ambito di applicazione di tale procedura e quelle connesse alle modifiche di cui al punto IS.I.OR.255, lettera b), sono approvate dall'autorità competente.

d) L'organizzazione può integrare l'ISMM con altri manuali o guide di gestione in suo possesso, a condizione che vi sia un chiaro riferimento incrociato che indichi quali parti dei manuali o delle guide di gestione corrispondono ai diversi requisiti contenuti nel presente allegato.

IS.I.OR.255 Modifiche del sistema di gestione della sicurezza delle informazioni

a) Le modifiche dell'ISMS possono essere gestite dall'organizzazione e notificate all'autorità competente in una procedura sviluppata dall'organizzazione stessa. Tale procedura è approvata dall'autorità competente.

b) Per quanto riguarda le modifiche dell'ISMS non contemplate dalla procedura di cui alla lettera a), l'organizzazione richiede e ottiene un'approvazione rilasciata dall'autorità competente.

Per quanto riguarda tali modifiche:

1) la domanda è presentata prima dell'effettuazione di ciascuna di tali modifiche, al fine di permettere all'autorità competente di stabilire il mantenimento della conformità al presente regolamento e di modificare, se necessario, il certificato dell'organizzazione e le relative condizioni di approvazione a esso allegate;

2) l'organizzazione mette a disposizione dell'autorità competente tutte le informazioni richieste per valutare le modifiche;

3) le modifiche sono attuate solo previa approvazione formale da parte dell'autorità competente;

4) l'organizzazione opera alle condizioni prescritte dall'autorità competente durante l'attuazione di tali modifiche.

IS.I.OR.260 Miglioramento continuo

a) L'organizzazione valuta, utilizzando adeguati indicatori di prestazione, l'efficacia e la maturità dell'ISMS. Tale valutazione è effettuata sulla base di un calendario predefinito dall'organizzazione o a seguito di un inconveniente nel settore della sicurezza delle informazioni.

b) Se si riscontrano carenze a seguito della valutazione effettuata conformemente alla lettera a), l'organizzazione adotta le misure di miglioramento necessarie per garantire che l'ISMS continui a rispettare i requisiti applicabili e mantenga i rischi per la sicurezza delle informazioni a un livello accettabile. L'organizzazione riesamina inoltre gli elementi dell'ISMS interessati dalle misure adottate.

ALLEGATO III

Gli allegati VI (parte ARA) e VII (parte ORA) del regolamento (UE) n. 1178/2011 sono così modificati:

1) l'allegato VI (parte ARA) è così modificato:

a) al punto ARA.GEN.125 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro deve fornire quanto prima all'Agenzia le informazioni rilevanti dal punto di vista della sicurezza, derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203.»;

b) dopo il punto ARA.GEN.135 è inserito il seguente punto ARA.GEN.135A:

«**ARA.GEN.135A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente deve attuare un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine deve coordinarsi con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia deve attuare un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto ARA.GEN.125, lettera c), e trasmettere senza indebito ritardo agli Stati membri e alla Commissione tutte le informazioni, incluse le raccomandazioni o le azioni correttive da adottare, che sono necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Al momento della ricezione delle informazioni di cui alle lettere a) e b), l'autorità competente deve adottare misure adeguate per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) Le misure adottate a norma della lettera c) devono essere immediatamente notificate a tutte le persone o organizzazioni tenute a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro deve inoltre notificare tali misure all'Agenzia e, qualora sia richiesta un'azione combinata, agli altri Stati membri interessati.»;

c) al punto ARA.GEN.200 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione stabilito e mantenuto dall'autorità competente deve essere conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

d) il punto ARA.GEN.205 è così modificato:

i) il titolo è sostituito dal seguente:

«**ARA.GEN.205 Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ORA.GEN.200A, l'autorità competente può assegnare compiti a enti qualificati conformemente al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. Nell'assegnare tali compiti, l'autorità competente si assicura che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dall'ente qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dall'ente qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto ARA.GEN.200, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

e) al punto ARA.GEN.300 è aggiunta la seguente lettera g):

«g) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ORA.GEN.200A, oltre a rispettare le lettere da a) a f), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

f) dopo il punto ARA.GEN.330 è inserito il seguente punto ARA.GEN.330A:

«**ARA.GEN.330A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente inserisce il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto ARA.GEN.300. Qualora si riscontri una non conformità, l'autorità competente informa l'organizzazione, richiede ulteriori modifiche e agisce in conformità al punto ARA.GEN.350.

b) Per quanto riguarda altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) al momento della ricezione della richiesta di modifica, prima di rilasciare l'approvazione l'autorità competente verifica che l'organizzazione sia conforme ai requisiti applicabili;

2) l'autorità competente stabilisce le condizioni alle quali l'organizzazione può operare durante l'attuazione della modifica;

3) se soddisfatta della conformità dell'organizzazione ai requisiti applicabili, l'autorità competente approva la modifica.»;

2) l'allegato VII (parte ORA) è così modificato:

il seguente punto ORA.GEN.200A è inserito dopo il punto ORA.GEN.200:

«**ORA.GEN.200A Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto ORA.GEN.200, l'organizzazione stabilisce, attua e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.».

ALLEGATO IV

L'allegato I (parte 21) del regolamento (UE) n. 748/2012 è così modificato:

1) l'indice è così modificato:

a) dopo il titolo 21.B.20 è inserito il titolo seguente:

«21.B.20A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea»;

b) il titolo della norma 21.B.30 è sostituito dal seguente:

«21.B.30 Assegnazione di compiti»;

c) dopo il titolo 21.B.240 è inserito il titolo seguente:

«21.B.240A Modifiche al sistema di gestione della sicurezza delle informazioni»;

d) dopo il titolo 21.B.435 è inserito il titolo seguente:

«21.B.435A Modifiche al sistema di gestione della sicurezza delle informazioni»;

2) al punto 21.B.15 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro deve fornire quanto prima all'Agenzia informazioni rilevanti dal punto di vista della sicurezza, derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.D.OR.230 dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645»;

3) dopo il punto 21.B.20 è inserito il seguente punto 21.B.20A:

«**21.B.20A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente deve attuare un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle imprese. A tal fine deve coordinarsi con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia deve attuare un sistema per analizzare in maniera adeguata tutte le informazioni rilevanti dal punto di vista della sicurezza ricevuta conformemente al punto 21.B.15, lettera c), e trasmettere senza indebito ritardo agli Stati membri e alla Commissione tutte le informazioni necessarie, incluse le raccomandazioni o le azioni correttive da intraprendere, affinché possano reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni (imprese) soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Non appena ricevute le informazioni di cui alle lettere a) e b), l'autorità competente deve adottare le misure adeguate per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) Le misure adottate conformemente alla lettera c) devono essere immediatamente notificate a tutte le persone o le organizzazioni (imprese) che devono rispettarle a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro deve inoltre notificare tali misure all'Agenzia e, nel caso in cui fosse necessaria un'azione combinata, agli altri Stati membri interessati.»;

4) al punto 21.B.25 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione istituito e mantenuto dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

5) il punto 21.B.30 è così modificato:

a) il titolo è sostituito dal seguente:

«21.B.30 Assegnazione di compiti»;

b) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'impresa ai punti 21.A.139A e 21.A.239A, l'autorità competente può assegnare compiti a soggetti qualificati in conformità alla lettera a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. Nell'assegnare tali compiti, l'autorità competente deve garantire che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'impresa;

3) il proprio sistema di gestione della sicurezza delle informazioni, istituito conformemente al punto 21.B.25, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

6) al punto 21.B.221 è aggiunta la seguente lettera g):

«g) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto 21.A.139A, oltre a rispettare le lettere da a) a f), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

7) dopo il punto 21.B.240 è inserito il seguente punto 21.B.240A:

«**21.B.240A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.D.OR.255, lettera a), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645, l'autorità competente deve inserire il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto 21.B.221. Qualora si riscontri una non conformità, l'autorità competente deve informare l'impresa, richiedere ulteriori modifiche e agire in conformità al punto 21.B.225.

b) Per quanto riguarda altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.D.OR.255, lettera b), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645:

1) al ricevimento della domanda di modifica, prima di rilasciare l'approvazione l'autorità competente deve verificare la conformità dell'impresa ai requisiti applicabili;

2) l'autorità competente deve stabilire le condizioni alle quali l'impresa può operare durante l'attuazione della modifica;

3) se convinta della conformità dell'impresa ai requisiti applicabili, l'autorità competente deve approvare la modifica.»;

8) al punto 21.B.431 è aggiunta la seguente lettera d):

«d) Per la certificazione e la sorveglianza della conformità dell'impresa al punto 21.A.239A, oltre a rispettare le lettere da a) a c), l'autorità competente rispetta i principi seguenti:

1) l'autorità competente deve riesaminare le interfacce e i rischi associati, individuati conformemente all'allegato (parte IS.D.OR), punto IS.D.OR.205, lettera b), del regolamento delegato (UE) 2022/1645 da ciascuna impresa soggetta alla sua sorveglianza;

2) qualora si riscontrino discrepanze nelle interfacce reciproche e nei rischi associati individuati da imprese diverse, l'autorità competente deve riesaminarle con le imprese interessate e, se necessario, segnalare le adeguate risultanze per garantire l'attuazione di azioni correttive;

3) qualora la documentazione esaminata a norma del punto 2) riveli l'esistenza di rischi significativi associati alle interfacce con imprese soggette alla sorveglianza di una diversa autorità competente nello stesso Stato membro, tale informazione deve essere comunicata all'autorità competente corrispondente.»;

9) dopo il punto 21.B.435 è inserito il seguente punto 21.B.435A:

«**21.B.435A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.D.OR.255, lettera a), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645, l'autorità competente deve inserire il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto 21.B.431. Se viene riscontrata una non conformità, l'autorità competente deve informare l'organizzazione, richiedere ulteriori modifiche e agire in conformità al punto 21.B.433.

b) Per quanto riguarda altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.D.OR.255, lettera b), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645:

1) al ricevimento della domanda di modifica, prima di rilasciare l'approvazione l'autorità competente deve verificare la conformità dell'impresa ai requisiti applicabili;

2) l'autorità competente deve stabilire le condizioni alle quali l'impresa può operare durante l'attuazione della modifica;

3) se convinta della conformità dell'impresa ai requisiti applicabili, l'autorità competente deve approvare la modifica.».

ALLEGATO V

Gli allegati II (parte ARO) e III (parte ORO) del regolamento (UE) n. 965/2012 sono così modificati:

1) l'allegato II (parte ARO) è così modificato:

a) al punto ARO.GEN.125 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro fornisce all'Agenzia il prima possibile le informazioni rilevanti dal punto di vista della sicurezza, provenienti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203.»;

b) dopo il punto ARO.GEN.135 è inserito il seguente punto ARO.GEN.135A:

«**ARO.GEN.135A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente pone in atto un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine si coordina con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia pone in atto un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto ARO.GEN.125, lettera c), e fornire agli Stati membri e alla Commissione, senza ulteriori ritardi, tutte le informazioni, incluse le raccomandazioni o le azioni correttive da adottare, che si rendono necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Al momento della ricezione delle informazioni di cui alle lettere a) e b), l'autorità competente adotta i provvedimenti adeguati per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) I provvedimenti intrapresi conformemente alla lettera c) sono immediatamente comunicati a tutte le persone o organizzazioni tenute a rispettarli a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro comunica i suddetti provvedimenti anche all'Agenzia e, nel caso in cui sia necessario un intervento combinato, agli altri Stati membri interessati.»;

c) al punto ARO.GEN.200 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione stabilito e mantenuto dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

d) il punto ARO.GEN.205 è così modificato:

i) il titolo è sostituito dal seguente:

«**ARO.GEN.205 Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ORO.GEN.200A, l'autorità competente può assegnare compiti a soggetti qualificati in conformità al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. In occasione dell'assegnazione dei compiti, l'autorità competente si accerta che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto ARO.GEN.200, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

e) al punto ARO.GEN.300 è aggiunta la seguente lettera g):

«g) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ORO.GEN.200A, oltre a rispettare le lettere da a) a f), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

f) dopo il punto ARO.GEN.330 è inserito il seguente punto ARO.GEN.330A:

«**ARO.GEN.330A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente inserisce il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto ARO.GEN.300. Qualora si riscontri una non conformità, l'autorità competente informa l'organizzazione, richiede ulteriori modifiche e agisce in conformità al punto ARO.GEN.350.

b) Per quanto riguarda le altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) all'atto della ricezione della domanda di modifica, prima di rilasciare l'approvazione l'autorità competente verifica la rispondenza dell'organizzazione ai requisiti applicabili;

2) l'autorità competente stabilisce le condizioni alle quali l'organizzazione può operare durante l'attuazione della modifica;

3) se convinta che organizzazione risponde ai requisiti applicabili, l'autorità competente approva la modifica.»;

2) l'allegato III (parte ORO) è così modificato:

dopo il punto ORO.GEN.200 è inserito il seguente punto ORO.GEN.200A:

«**ORO.GEN.200A Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto ORO.GEN.200, l'operatore deve stabilire, attuare e mantenere un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.».

ALLEGATO VI

L'allegato II (parte ADR.AR) del regolamento (UE) n. 139/2014 è così modificato:

1) al punto ADR.AR.A.025 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro deve fornire quanto prima all'Agenzia informazioni rilevanti dal punto di vista della sicurezza, derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.D.OR.230 dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645.»;

2) dopo il punto ADR.AR.A.030 è inserito il seguente punto ADR.AR.A.030A:

«**ADR.AR.A.030A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente pone in atto un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine si coordina con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia attua un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto ADR.AR.A.025, lettera c), e fornisce agli Stati membri e alla Commissione, senza indebiti ritardi, tutte le informazioni, incluse le raccomandazioni o le azioni correttive da intraprendere, che sono necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Al momento della ricezione delle informazioni di cui alle lettere a) e b), l'autorità competente adotta provvedimenti adeguati per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) I provvedimenti adottati in conformità alla lettera c) vengono immediatamente comunicati a tutte le persone o organizzazioni tenute a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro comunica tali provvedimenti anche all'Agenzia e, nel caso in cui fosse richiesta un'azione combinata, agli altri Stati membri interessati.»;

3) al punto ADR.AR.B.005 è aggiunta la seguente lettera d):

«d) Oltre ai requisiti di cui alla lettera a), il sistema di gestione stabilito e mantenuto dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

4) il punto ADR.AR.B.010 è così modificato:

i) il titolo è sostituito dal seguente:

«**ADR.AR.B.010 Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ADR.OR.D.005A, l'autorità competente può assegnare compiti a organizzazioni riconosciute in conformità alla lettera a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. In occasione dell'assegnazione dei compiti, l'autorità competente si accerta che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dall'organizzazione riconosciuta o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dall'organizzazione riconosciuta o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto ADR.AR.B.005, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

5) al punto ADR.AR.C.005 è aggiunta la seguente lettera f):

«f) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ADR.OR.D.005A, oltre a rispettare le lettere da a) a e), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

6) dopo il punto ADR.AR.C.040 è inserito il seguente punto ADR.AR.C.040A:

«**ADR.AR.C.040A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.D.OR.255, lettera a), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645, l'autorità competente deve inserire il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto ADR.AR.C.005. Qualora si riscontri una non conformità, l'autorità competente informa l'organizzazione, richiede ulteriori modifiche e agisce in conformità al punto ADR.AR.C.055.

b) Per quanto riguarda altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.D.OR.255, lettera b), dell'allegato (parte IS.D.OR) del regolamento delegato (UE) 2022/1645:

1) all'atto della ricezione di una domanda di modifica, prima di rilasciare l'approvazione l'autorità competente verifica la conformità dell'organizzazione ai requisiti applicabili;

2) l'autorità competente stabilisce le condizioni alle quali l'organizzazione può operare durante l'attuazione della modifica;

3) se convinta della conformità dell'organizzazione ai requisiti applicabili, l'autorità competente approva la modifica.».

ALLEGATO VII

Gli allegati II (parte 145), III (parte 66) e V *quater* (parte CAMO) del regolamento (UE) n. 1321/2014 sono così modificati:

1) l'allegato II (parte 145) è così modificato:

a) l'indice è così modificato:

i) dopo il titolo 145.A.200 è inserito il titolo seguente:

«145.A.200A Sistema di gestione della sicurezza delle informazioni»;

ii) dopo il titolo 145.B.135 è inserito il titolo seguente:

«145.B.135A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea»;

iii) il titolo della norma 145.B.205 è sostituito dal seguente:

«145.B.205 Assegnazione dei compiti»;

iv) dopo il titolo 145.B.330 è inserito il titolo seguente:

«145.B.330A Modifiche al sistema di gestione della sicurezza delle informazioni»;

b) dopo il punto 145.A.200 è inserito il seguente punto 145.A.200A:

«145.A.200A **Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto 145.A.200, l'impresa deve istituire, realizzare e mantenere un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

c) al punto 145.B.125 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro deve fornire quanto prima all'Agenzia tutte le informazioni rilevanti dal punto di vista della sicurezza derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203.»;

d) dopo il punto 145.B.135 è inserito il seguente punto 145.B.135A:

«145.B.135A **Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente deve attuare un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle imprese. A tal fine si deve coordinare con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia deve attuare un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto 145.B.125, lettera c), e deve trasmettere immediatamente agli Stati membri e alla Commissione tutte le informazioni, incluse le raccomandazioni o le azioni correttive da intraprendere, necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni (imprese) soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Non appena ricevute le informazioni di cui alle lettere a) e b), l'autorità competente deve adottare le misure adeguate per affrontare il potenziale impatto sulla sicurezza aerea dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni.

d) Le misure adottate conformemente alla lettera c) devono essere immediatamente notificate a tutte le persone o organizzazioni (imprese) tenute a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente deve inoltre notificare tali misure all'Agenzia e, nel caso in cui fosse necessaria un'azione combinata, agli altri Stati membri interessati.»;

e) al punto 145.B.200 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione istituito e mantenuto dall'autorità competente deve essere conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

f) il punto 145.B.205 è così modificato:

i) il titolo è sostituito dal seguente:

«145.B.205 **Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'impresa al punto 145.A.200A, l'autorità competente può assegnare compiti a soggetti qualificati in conformità al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. Nell'assegnare tali compiti, l'autorità competente deve assicurarsi che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, istituito conformemente al punto 145.B.200, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

g) al punto 145.B.300 è aggiunta la seguente lettera g):

«g) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto 145.A.200A, oltre a rispettare le lettere da a) a f), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

h) dopo il punto 145.B.330 è inserito il seguente punto 145.B.330A:

«145.B.330A **Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente deve includere l'analisi delle modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto 145.B.300. Qualora siano riscontrate non conformità, l'autorità competente deve informare l'impresa, richiedere ulteriori modifiche e agire in conformità al punto 145.B.350.

b) Per quanto riguarda le altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) al ricevimento di una richiesta relativa a una modifica, l'autorità competente deve verificare che l'impresa sia conforme ai requisiti applicabili prima di rilasciare l'approvazione;

2) l'autorità competente deve definire le condizioni alle quali l'impresa può operare durante l'attuazione della modifica;

3) se è convinta che l'impresa risponde ai requisiti applicabili, l'autorità competente deve approvare la modifica.»;

2) l'allegato III (parte 66) è così modificato:

a) nell'indice, dopo il titolo 66.B.10 è inserito il titolo seguente:

«66.B.15 Sistema di gestione della sicurezza delle informazioni»;

b) dopo il punto 66.B.10 è inserito il seguente punto 66.B.15:

«66.B.15 **Sistema di gestione della sicurezza delle informazioni**

L'autorità competente deve istituire, attuare e mantenere un sistema di gestione della sicurezza delle informazioni in conformità all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

3) l'allegato V quater (parte CAMO) è così modificato:

a) l'indice è così modificato:

i) dopo il titolo CAMO.A.200 è inserito il titolo seguente:

«CAMO.A.200A Sistema di gestione della sicurezza delle informazioni»;

ii) dopo il titolo CAMO.B.135 è inserito il titolo seguente:

«CAMO.B.135A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea»;

iii) il titolo della norma CAMO.B.205 è sostituito dal seguente:

«CAMO.B.205 Assegnazione dei compiti»;

iv) dopo il titolo CAMO.B.330 è inserito il titolo seguente:

«CAMO.B.330A Modifiche al sistema di gestione della sicurezza delle informazioni»;

b) dopo il punto CAMO.A.200 è inserito il seguente punto CAMO.A.200A:

«CAMO.A.200A **Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto CAMO.A.200, l'impresa stabilisce, attua e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

c) al punto CAMO.B.125 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro fornisce quanto prima all'Agenzia informazioni rilevanti dal punto di vista della sicurezza, derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) al del regolamento di esecuzione (UE) 2023/203.»;

d) il punto seguente CAMO.B.135A è inserito dopo il punto CAMO.B.135:

«CAMO.B.135A **Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente deve attuare un sistema per raccogliere, analizzare e diffondere in modo appropriato le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine si coordina con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia attua un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto CAMO.B.125, lettera c), e trasmette immediatamente agli Stati membri e alla Commissione tutte le informazioni, incluse le raccomandazioni o le azioni correttive da intraprendere, necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni (imprese) soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Non appena ricevute le informazioni di cui alle lettere a) e b), l'autorità competente adotta le misure adeguate per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) Le misure adottate conformemente alla lettera c) sono immediatamente notificate a tutte le persone o organizzazioni (imprese) tenute a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro deve inoltre notificare tali misure all'Agenzia e, nel caso in cui fosse necessaria un'azione combinata, agli altri Stati membri interessati.»;

e) al punto CAMO.B.200 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione stabilito e mantenuto dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

f) il punto CAMO.B.205 è così modificato:

i) il titolo è sostituito dal seguente:

«CAMO.B.205 **Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto CAMO.A.200A, l'autorità competente può assegnare compiti a soggetti qualificati in conformità al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. Nell'assegnare tali compiti, l'autorità competente si assicura che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto CAMO.B.200, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

g) al punto CAMO.B.300 è aggiunta la seguente lettera g):

«g) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto CAMO.A.200A, oltre a rispettare le lettere da a) a f), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

h) dopo il punto CAMO.B.330 è inserito il seguente punto CAMO.B.330A:

«CAMO.B.330A **Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente inserisce il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto CAMO.B.300. Qualora si riscontri una non conformità, l'autorità competente informa l'impresa, richiede ulteriori modifiche e agisce in conformità al punto CAMO.B.350.

b) Per quanto riguarda le altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) al ricevimento di una richiesta relativa ad una modifica, l'autorità competente verifica che l'impresa sia conforme ai requisiti applicabili prima di rilasciare l'approvazione;

2) l'autorità competente stabilisce le condizioni alle quali l'impresa può operare durante l'attuazione della modifica;

3) se convinta che l'impresa risponde ai requisiti applicabili, l'autorità competente approva la modifica.».

ALLEGATO VIII

Gli allegati II (parte ATCO.AR) e III (parte ATCO.OR) del regolamento (UE) 2015/340 sono così modificati:

1) l'allegato II (parte ATCO.AR) è così modificato:

a) al punto ATCO.AR.A.020 è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro fornisce quanto prima all'Agenzia informazioni rilevanti sotto il profilo della sicurezza, ricavate dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203.»;

b) dopo il punto ATCO.AR.A.025 è inserito il seguente punto ATCO.AR.A.025A:

«**ATCO.AR.A.025A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente deve attuare un sistema per raccogliere, analizzare e diffondere in maniera adeguata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine si coordina con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia attua un sistema per analizzare in maniera adeguata tutte le pertinenti informazioni rilevanti sotto il profilo della sicurezza ricevute conformemente al punto ATCO.AR.A.020, e trasmette immediatamente agli Stati membri e alla Commissione tutte le informazioni, incluse le raccomandazioni o le azioni correttive da intraprendere, necessarie per reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Al momento della ricezione delle informazioni di cui alle lettere a) e b), l'autorità competente deve prendere le misure adeguate per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) Le misure adottate di cui alla lettera c) devono essere immediatamente notificate a tutte le persone o organizzazioni che devono conformarsi ad esse a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro deve inoltre notificare tali misure all'Agenzia e, nel caso in cui fosse necessaria un'azione combinata, agli altri Stati membri interessati.»;

c) al punto ATCO.AR.B.001 è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione istituito e attuato dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

d) il punto ATCO.AR.B.005 è così modificato:

i) il titolo è sostituito dal seguente:

«**ATCO.AR.B.005 Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ATCO.OR.C.001A, l'autorità competente può assegnare compiti a soggetti qualificati in conformità al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza nello Stato membro. Nell'assegnare tali compiti, l'autorità competente si assicura che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto qualificato o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto qualificato o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto ATCO.AR.B.001, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

e) al punto ATCO.AR.C.001 è aggiunta la seguente lettera f):

«f) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ATCO.OR.C.001A, oltre a rispettare le lettere da a) a e), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

f) dopo il punto ATCO.AR.E.010 è inserito il seguente punto ATCO.AR.E.010A:

«**ATCO.AR.E.010A Modifiche al sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente inserisce il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto ATCO.AR.C.001. Qualora si riscontri una non conformità, l'autorità competente informa l'organizzazione, richiede ulteriori modifiche e agisce in conformità al punto ATCO.AR.C.010.

b) Per quanto riguarda le altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) al momento del ricevimento di una domanda di modifica, prima di rilasciare l'approvazione l'autorità competente verifica la conformità dell'organizzazione ai requisiti applicabili;

2) l'autorità competente stabilisce le condizioni alle quali l'organizzazione può operare durante l'attuazione della modifica;

3) se è convinta della conformità dell'organizzazione ai requisiti applicabili, l'autorità competente approva la modifica»;

2) l'allegato III (parte ATCO.OR) è così modificato:

il seguente punto ATCO.OR.C.001A è inserito dopo il punto ATCO.OR.C.001:

«**ATCO.OR.C.001 Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto ATCO.OR.C.001, l'organizzazione di addestramento devono stabilire, attuare e mantenere un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.».

ALLEGATO IX

Gli allegati II (parte ATM/ANS.AR) e III (parte ATM/ANS.OR) del regolamento di esecuzione (UE) 2017/373 sono così modificati:

1) l'allegato II (parte ATM/ANS.OR) è così modificato:

a) al punto ATM/ANS.AR.A.020, è aggiunta la seguente lettera c):

«c) L'autorità competente dello Stato membro fornisce quanto prima all'Agenzia informazioni rilevanti dal punto di vista della sicurezza, derivanti dalle relazioni sulla sicurezza delle informazioni ricevute a norma del punto IS.I.OR.230 dell'allegato II (parte IS.I.OR) al del regolamento di esecuzione (UE) 2023/203.»;

b) il punto seguente ATM/ANS.AR.A.025A è inserito dopo il punto ATM/ANS.AR.A.025:

«**ATM/ANS.AR.A.025A Reazione immediata a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un impatto sulla sicurezza aerea**

a) L'autorità competente attua un sistema per raccogliere, analizzare e divulgare in maniera appropriata le informazioni relative agli inconvenienti e alle vulnerabilità riguardanti la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea segnalati dalle organizzazioni. A tal fine si coordina con eventuali altre autorità pertinenti responsabili della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro, per migliorare il coordinamento e la compatibilità dei sistemi di segnalazione.

b) L'Agenzia attua un sistema per analizzare in maniera appropriata tutte le pertinenti informazioni rilevanti dal punto di vista della sicurezza ricevute conformemente al punto ATM/ANS.AR.A.020, lettera c), e fornisce immediatamente agli Stati membri e alla Commissione tutte le informazioni necessarie, incluse le raccomandazioni o le azioni correttive da intraprendere, per poter reagire tempestivamente a un inconveniente o a una vulnerabilità riguardante la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea concernente i prodotti, le parti, gli equipaggiamenti non installati, le persone o le organizzazioni soggette al regolamento (UE) 2018/1139 e ai relativi atti delegati e di esecuzione.

c) Al ricevimento delle informazioni di cui alle lettere a) e b), l'autorità competente adotta misure adeguate per affrontare il potenziale impatto dell'inconveniente o della vulnerabilità riguardante la sicurezza delle informazioni sulla sicurezza aerea.

d) Le misure adottate conformemente alla lettera c) sono immediatamente notificate a tutte le persone o organizzazioni tenute a rispettarle a norma del regolamento (UE) 2018/1139 e dei relativi atti delegati e di esecuzione. L'autorità competente dello Stato membro notifica inoltre tali misure all'Agenzia e, nel caso in cui fosse necessaria un'azione combinata, agli altri Stati membri interessati.»;

c) al punto ATM/ANS.AR.B.001, è aggiunta la seguente lettera e):

«e) Oltre ai requisiti di cui alla lettera a), il sistema di gestione stabilito e mantenuto dall'autorità competente è conforme all'allegato I (parte IS.AR) del regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.»;

d) il punto ATM/ANS.AR.B.005 è così modificato:

i) il titolo è sostituito dal seguente:

«**ATM/ANS.AR.B.005 Assegnazione dei compiti**»;

ii) è aggiunta la seguente lettera c):

«c) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ATM/ANS.OR.B.005A, l'autorità competente può assegnare mansioni a soggetti riconosciuti in conformità al punto a), o a qualsiasi autorità pertinente responsabile della sicurezza delle informazioni o della cibersicurezza all'interno dello Stato membro. Nell'assegnare tali compiti, l'autorità competente si assicura che:

1) tutti gli aspetti legati alla sicurezza aerea siano coordinati e presi in considerazione dal soggetto riconosciuto o dall'autorità pertinente;

2) i risultati delle attività di certificazione e sorveglianza svolte dal soggetto riconosciuto o dall'autorità pertinente siano integrati nei fascicoli complessivi di certificazione e sorveglianza dell'organizzazione;

3) il proprio sistema di gestione della sicurezza delle informazioni, stabilito conformemente al punto ATM/ANS.AR.B.001, lettera e), includa tutti i compiti di certificazione e di sorveglianza continua svolti per suo conto.»;

e) al punto ATM/ANS.AR.C.010, è aggiunta la seguente lettera d):

«d) Per quanto riguarda la certificazione e la sorveglianza della conformità dell'organizzazione al punto ATM/ANS.OR.B.005A, oltre a rispettare le lettere da a) a c), l'autorità competente riesamina qualsiasi approvazione concessa a norma del punto IS.I.OR.200, lettera e), del presente regolamento o del punto IS.D.OR.200, lettera e), del regolamento delegato (UE) 2022/1645 a seguito del ciclo di audit di supervisione applicabile e ogniqualvolta siano attuate modifiche nell'ambito del lavoro dell'organizzazione.»;

f) il punto seguente ATM/ANS.AR.C.025A è inserito dopo il punto ATM/ANS.AR.C.025:

«**ATM/ANS.AR.C.025A Modifiche del sistema di gestione della sicurezza delle informazioni**

a) Per quanto riguarda le modifiche gestite e notificate all'autorità competente in conformità alla procedura di cui al punto IS.I.OR.255, lettera a), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203, l'autorità competente inserisce il riesame di tali modifiche nella sua sorveglianza continua, conformemente ai principi stabiliti al punto ATM/ANS.AR.C.010. Qualora si riscontri una non conformità, l'autorità competente informa l'organizzazione, richiede ulteriori modifiche e agisce in conformità al punto ATM/ANS.AR.C.050.

b) Per quanto riguarda le altre modifiche per le quali occorre una richiesta di approvazione in conformità al punto IS.I.OR.255, lettera b), dell'allegato II (parte IS.I.OR) del regolamento di esecuzione (UE) 2023/203:

1) al ricevimento della domanda di modifica, prima di rilasciare l'approvazione l'autorità competente verifica la conformità dell'organizzazione ai requisiti applicabili;

2) l'autorità competente stabilisce le condizioni alle quali l'organizzazione può operare durante l'attuazione della modifica;

3) se è convinta della conformità dell'organizzazione ai requisiti applicabili, l'autorità competente approva la modifica.»;

2) l'allegato III (parte ATM/ANS.OR) è così modificato:

a) il punto seguente ATM/ANS.OR.B.005A è inserito dopo il punto ATM/ANS.OR.B.005:

«**ATM/ANS.OR.B.005 Sistema di gestione della sicurezza delle informazioni**

Oltre al sistema di gestione di cui al punto ATM/ANS.OR.B.005, il fornitore di servizi istituisce, attua e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento di esecuzione (UE) 2023/203 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea»;

b) il punto ATM/ANS.OR.D.010 è sostituito dal seguente:

«**ATM/ANS.OR.D.010 Gestione della sicurezza (*security*)**

a) Come parte integrante del loro sistema di gestione, secondo quanto previsto al punto ATM/ANS.OR.B.005, i fornitori di servizi di navigazione aerea e di gestione dei flussi di traffico aereo e il gestore della rete istituiscono un sistema di gestione della sicurezza (*security*) al fine di assicurare:

1) la sicurezza dei loro impianti e del loro personale in modo da prevenire qualsiasi indebita interferenza nella fornitura dei servizi;

2) la sicurezza dei dati operativi che ricevono, producono o utilizzano, di modo che il loro accesso sia riservato alle sole persone autorizzate.

b) Il sistema di gestione della sicurezza (*security*) definisce:

1) i processi e le procedure relative alla valutazione e alla riduzione del rischio per la sicurezza, al controllo e al miglioramento della sicurezza, alle valutazioni della sicurezza e alla diffusione degli insegnamenti tratti;

2) i mezzi per individuare, monitorare e rilevare le violazioni della sicurezza e allertare il personale con opportuni avvisi;

3) i mezzi per contenere gli effetti delle violazioni della sicurezza e individuare le misure di ripristino e le procedure di attenuazione dei rischi per evitare che tali eventi si ripetano.

c) I fornitori di servizi di navigazione aerea e di gestione dei flussi di traffico aereo e il gestore della rete garantiscono che il loro personale sia dotato di nulla osta di sicurezza, se del caso, e si coordinano con le competenti autorità civili e militari per garantire la sicurezza degli impianti, del personale e dei dati.

d) Gli aspetti relativi alla sicurezza delle informazioni devono essere gestiti conformemente al punto ATM.ANS.OR.B.005A.».