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

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 19, paragrafo 1, lettera g), e l'articolo 39, paragrafo 1, lettera b),

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 di progettazione e produzione 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 VII, punti 2.2.1 e 5.2, del regolamento (UE) 2018/1139, i gestori aeroportuali e le organizzazioni responsabili della fornitura di servizi di gestione del piazzale devono realizzare e mantenere un sistema di gestione per gestire i rischi in materia di sicurezza.

(3) I rischi in materia di sicurezza di cui ai considerando 1 e 2 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 dalle organizzazioni di cui ai considerando 1 e 2 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 dal momento che gli attuali sistemi informativi stanno diventando sempre più interconnessi e sempre più bersaglio di attori malintenzionati.

(4) 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.

(5) Un numero significativo di imprese 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.

(6) È pertanto opportuno stabilire requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea.

(7) È essenziale che tali requisiti riguardino i diversi 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 imprese che sono già tenute a disporre un sistema di gestione conformemente alla vigente normativa dell'Unione in materia di sicurezza aerea.

(8) I requisiti di cui al presente regolamento dovrebbero essere applicati in modo 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.

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

(9) 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 ([2]) e all'articolo 14 della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([3]).

(10) La definizione di sicurezza delle informazioni utilizzata ai fini del presente atto giuridico non dovrebbe essere interpretata come divergente dalla definizione di sicurezza delle reti e dei sistemi informativi di cui alla direttiva 2016/1148.

(11) Al fine di evitare la duplicazione dei requisiti giuridici, qualora le imprese contemplate dal presente regolamento siano già soggette a obblighi di sicurezza derivanti da altri atti dell'Unione di cui al considerando 9, 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.

(12) Le imprese di cui al presente regolamento che sono già soggette agli obblighi di sicurezza derivanti dal regolamento di esecuzione (UE) 2015/1998 dovrebbero inoltre conformarsi ai requisiti di cui all'allegato I (parte IS.D.OR.230 «Sistema di segnalazione esterna della sicurezza delle informazioni») del presente regolamento, poiché il regolamento (UE) 2015/1998 non contiene disposizioni relative alla segnalazione esterna degli inconvenienti per la sicurezza delle informazioni.

(13) I regolamenti di esecuzione (UE) n. 748/2012 ([4]) e (UE) n. 139/2014 della Commissione ([5]) dovrebbero essere modificati al fine di stabilire un legame tra i sistemi di gestione prescritti dai regolamenti sopra elencati e i requisiti di gestione della sicurezza delle informazioni prescritti dal presente regolamento.

(14) Al fine di fornire alle imprese il tempo sufficiente per garantire la conformità alle nuove norme e procedure introdotte dal presente regolamento, è opportuno che il presente regolamento si applichi a decorrere da tre anni dalla data di entrata in vigore.

(15) I requisiti stabiliti dal presente regolamento si basano sul parere n. 03/2021 ([6]), emesso dall'Agenzia in conformità all'articolo 75, paragrafo 2, lettere b) e c), e dell'articolo 76, paragrafo 1, del regolamento (UE) 2018/1139.

(16) Conformemente all'articolo 128, paragrafo 4, del regolamento (UE) 2018/1139, la Commissione ha consultato gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([7]),

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento stabilisce i requisiti che devono essere soddisfatti dalle imprese di cui all'articolo 2 al fine di 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, nonché 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, rispondere a tali inconvenienti e provvedere al ripristino.

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

([6]) https://www.easa.europa.eu/document-library/opinions.

([7]) GU L 123 del 12.5.2016, pag. 1.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica alle seguenti imprese:

a) le imprese di produzione e le imprese di progettazione soggette all'allegato I (parte 21), sezione A, capitoli G e J, del regolamento (UE) n. 748/2012, ad eccezione delle imprese di progettazione e di produzione che partecipano esclusivamente alla progettazione e/o alla produzione di aeromobili ELA2, quali definiti all'articolo 1, paragrafo 2, lettera j), del regolamento (UE) n. 748/2012;

b) i gestori aeroportuali e i fornitori di servizi di gestione del piazzale soggetti all'allegato III «Parte requisiti per l'organizzazione (Parte-ADR.OR)» del regolamento (UE) n. 139/2014.

2. 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 applicano le definizioni seguenti:

1) «sicurezza delle informazioni»: la salvaguardia 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 effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi quale definito 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;

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

Obblighi derivanti da altre normative dell'Unione

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

2. Se un'impresa di cui all'articolo 2 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 ([8]), 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.D.OR.230 dell'allegato del presente regolamento che è da rispettare.

([8]) 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).

3. La Commissione, previa consultazione dell'AESA 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 gli obblighi di cui alla direttiva (UE) 2016/1148.

Articolo 5

Autorità competente

1. L'autorità responsabile della certificazione e del controllo della conformità al presente regolamento è:

a) per quanto riguarda le imprese di cui all'articolo 2, lettera a), l'autorità competente designata conformemente all'allegato I (parte 21) del regolamento (UE) n. 748/2012;

b) per quanto riguarda le imprese di cui all'articolo 2, lettera b), l'autorità competente designata conformemente all'allegato III (Parte-ADR.OR) del regolamento (UE) n. 139/2014.

2. Ai fini del presente regolamento gli Stati membri possono designare un'entità indipendente e autonoma per svolgere il ruolo e le 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 supervisione efficace di tutti i requisiti che l'impresa deve soddisfare.

Articolo 6

Modifica del regolamento (UE) n. 748/2012

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.A.139 è inserito il titolo seguente:

      «**21.A.139 A Sistema di gestione della sicurezza delle informazioni**»;

   b) dopo il titolo 21.A.239 è inserito il titolo seguente:

      «**21.A.239 A Sistema di gestione della sicurezza delle informazioni**»;

2) il seguente punto 21.A.139 A è inserito dopo il punto 21.A.139:

   «**21.A.139 A Sistema di gestione della sicurezza delle informazioni**

   Oltre al sistema di gestione della produzione di cui al punto 21.A.139, l'impresa di produzione istituisce, realizza e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento delegato (UE) 2022/1645 della Commissione (*) al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.

   (*) 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)»;

3) il seguente punto 21.A.239 A è inserito dopo il punto 21.A.239:

   «**21.A.239 A Sistema di gestione della sicurezza delle informazioni**

   Oltre al sistema di gestione del progetto di cui al punto 21.A.239, l'impresa di progettazione istituisce, realizza e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento delegato (UE) 2022/1645 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.».

Articolo 7

Modifica del regolamento (UE) n. 139/2014

L'allegato III (Parte-ADR.OR) del regolamento (UE) n. 139/2014 è così modificato:

1) la seguente norma ADR.OR.D.005 A è inserita dopo la norma ADR.OR.D.005:

«**ADR.OR.D.005 A Sistema di gestione della sicurezza delle informazioni**

Il gestore aeroportuale istituisce, attua e mantiene un sistema di gestione della sicurezza delle informazioni conformemente al regolamento delegato (UE) 2022/1645 della Commissione (*) al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.

(*) 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)»;

2) la norma ADR.OR.D.007 è sostituita dalla seguente:

«**ADR.OR.D.007 Gestione dei dati aeronautici e delle informazioni aeronautiche**

a) Nell'ambito del suo sistema di gestione, il gestore aeroportuale deve attuare e mantenere un sistema di gestione della qualità che comprenda:

1) le sue attività sui dati aeronautici;

2) le sue attività di fornitura di informazioni aeronautiche.

b) Nell'ambito del suo sistema di gestione, il gestore aeroportuale deve istituire un sistema di gestione della sicurezza per garantire la sicurezza dei dati operativi che riceve, o produce, o impiega in altro modo, in maniera tale che l'accesso a tali dati operativi sia limitato a coloro che sono stati autorizzati.

c) Il sistema di gestione della sicurezza deve definire i seguenti elementi:

1) le procedure relative alla valutazione e all'attenuazione dei rischi per la sicurezza dei dati, al monitoraggio e al miglioramento della sicurezza, al riesame della sicurezza e alla diffusione degli insegnamenti tratti;

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

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

d) Il gestore aeroportuale deve garantire che il suo personale abbia ricevuto il nulla osta di sicurezza per quanto riguarda la sicurezza dei dati aeronautici.

e) Gli aspetti relativi alla sicurezza delle informazioni devono essere gestiti conformemente alla norma ADR.OR.D.005 A.»;

3) la seguente norma ADR.OR.F.045 A è inserita dopo la norma ADR.OR.F.045:

«**ADR.OR.F.045 A Sistema di gestione della sicurezza delle informazioni**

L'impresa responsabile della fornitura di servizi di gestione del piazzale deve istituire, attuare e mantenere un sistema di gestione della sicurezza delle informazioni conformemente al regolamento delegato (UE) 2022/1645 al fine di garantire la corretta gestione dei rischi per la sicurezza delle informazioni che possono avere un impatto sulla sicurezza aerea.».

Articolo 8

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

Esso si applica a decorrere dal 16 ottobre 2025.

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

Fatto a Bruxelles, il 14 luglio 2022

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

SICUREZZA DELLE INFORMAZIONI — REQUISITI PER L'IMPRESA

[PARTE-IS.D.OR]

IS.D.OR.100 Ambito di applicazione

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

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

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

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

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

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

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

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

IS.D.OR.240 Requisiti relativi al personale

IS.D.OR.245 Conservazione dei registri

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

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

IS.D.OR.260 Miglioramento continuo

IS.D.OR.100 Ambito di applicazione

La presente parte stabilisce i requisiti che le imprese di cui all'articolo 2 del presente regolamento devono soddisfare.

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

a) Al fine di conseguire gli obiettivi di cui all'articolo 1, l'impresa 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'impresa 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.D.OR.205;

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

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

   5) definire e attuare, conformemente al punto IS.D.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.D.OR.205, lettera e), nonché rispondere a tali inconvenienti per la sicurezza delle informazioni 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.D.OR.225, per rispondere alle non conformità notificate dall'autorità competente;

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

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

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

11) soddisfare i requisiti per la conservazione dei registri di cui al punto IS.D.OR.245;

12) controllare la conformità dell'impresa ai requisiti del presente regolamento e fornire un riscontro sulle non conformità al dirigente responsabile o, nel caso delle imprese di progettazione, al capo dell'impresa di progettazione, 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'impresa potrebbe aver ricevuto da altre imprese, a seconda del relativo livello di sensibilità.

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

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

d) I processi, le procedure, i ruoli e le responsabilità stabiliti dall'impresa per conformarsi al punto IS.D.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'impresa.

e) Fatto salvo l'obbligo di rispettare gli obblighi di segnalazione di cui al regolamento (UE) n. 376/2014 ([1]) e i requisiti di cui al punto IS.D.OR.200, lettera a), punto 13), l'impresa può essere autorizzata dall'autorità competente a non attuare i requisiti di cui alle lettere da a) a d) e i relativi requisiti di cui ai punti da IS.D.OR.205 a IS.D.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'impresa o da un terzo conformemente al punto IS.D.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'impresa.

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

a) L'impresa 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'impresa, 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'impresa individua le interfacce che ha con altre imprese 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'impresa individua i rischi per la sicurezza delle informazioni che possono avere un potenziale impatto sulla sicurezza aerea. Per ogni rischio individuato l'impresa:

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

([1]) Regolamento (UE) n. 376/2014 del Parlamento europeo e del Consiglio, del 3 aprile 2014, concernente la segnalazione, l'analisi e il monitoraggio di eventi nel settore dell'aviazione civile, che modifica il regolamento (UE) n. 996/2010 del Parlamento europeo e del Consiglio e che abroga la direttiva 2003/42/CE del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 1321/2007 e (CE) n. 1330/2007 della Commissione (GU L 122 del 24.4.2014, pag. 18).

2) associa ciascun rischio e il suo livello all'elemento o all'interfaccia corrispondente 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'impresa dispone di un processo operativo di gestione dei rischi strutturato e ripetibile, l'impresa è in grado di stabilire se il rischio è accettabile o deve essere trattato conformemente al punto IS.D.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 imprese di cui alla lettera b).

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

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'impresa e le altre imprese, 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.D.OR.210 Trattamento dei rischi per la sicurezza delle informazioni

a) L'impresa elabora misure per affrontare i rischi inaccettabili individuati conformemente al punto IS.D.OR.205, le attua tempestivamente e ne verifica l'efficacia nel tempo. Tali misure consentono all'impresa 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.D.OR.240, lettere a) e b), e gli altri membri del personale interessati dell'impresa sono informati dell'esito della valutazione dei rischi effettuata conformemente al punto IS.D.OR.205, dei corrispondenti scenari di minaccia e delle misure da attuare.

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

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

a) L'impresa 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.D.OR.230.

b) Tale sistema e il processo di cui al punto IS.D.OR.220 consentono all'impresa 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.D.OR.205 e IS.D.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'impresa 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'impresa coopera alle indagini con qualsiasi altra impresa che fornisca un contributo significativo alla sicurezza delle informazioni delle proprie attività.

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

IS.D.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.D.OR.205 e dell'esito del trattamento dei rischi effettuato conformemente al punto IS.D.OR.210, l'impresa 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'impresa 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'impresa attua misure per rispondere a qualsiasi evento individuato in conformità alla lettera a), che può trasformarsi o si è trasformato in un inconveniente per la sicurezza delle informazioni. Tali misure di risposta consentono all'impresa 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.D.OR.205, lettera a).

c) L'impresa attua misure volte al ripristino dopo inconvenienti per la sicurezza delle informazioni, comprese, se necessario, misure di emergenza. Tali misure di ripristino consentono all'impresa 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.D.OR.205, lettera a), entro un tempo di recupero precedentemente definito dall'impresa.

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

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

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.D.OR.230 Sistema di segnalazione esterna della sicurezza delle informazioni

a) L'impresa 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'impresa.

b) Fatti salvi gli obblighi del regolamento (UE) n. 376/2014, l'impresa 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'impresa segnala il fatto anche al titolare dell'approvazione del progetto;

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

c) L'impresa 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'impresa responsabile della progettazione del sistema o del componente, non appena l'impresa 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'impresa responsabile della progettazione del sistema o del componente il prima possibile, ma non oltre 72 ore dal momento in cui l'impresa 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'impresa;

3) una segnalazione di follow-up è presentata all'autorità competente e, se del caso, al titolare dell'approvazione del progetto o all'impresa responsabile della progettazione del sistema o del componente, fornendo i dettagli delle azioni che l'impresa 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.D.OR.235 Appalto delle attività di gestione della sicurezza delle informazioni

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

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

IS.D.OR.240 Requisiti relativi al personale

a) Il dirigente responsabile dell'impresa o, nel caso delle imprese di progettazione, il capo dell'impresa di progettazione, designato a norma del regolamento (UE) n. 748/2012 e del regolamento (UE) n. 139/2014 di cui all'articolo 2, paragrafo 1, lettere a) e b), del presente regolamento, ha l'autorità giuridica per garantire che tutte le attività richieste dal presente regolamento possano essere finanziate e svolte. 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.D.OR.200, lettera a), punto 1);

3) dimostra una comprensione di base del presente regolamento.

b) Il dirigente responsabile o, nel caso delle imprese di progettazione, il capo dell'impresa di progettazione nomina una persona o un gruppo di persone che garantisca la conformità dell'impresa ai requisiti del presente regolamento, e definisce la portata della loro autorità. Tale persona o gruppo di persone riferisce direttamente al dirigente responsabile o, nel caso delle imprese di progettazione, al capo dell'impresa di progettazione 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 o, nel caso delle imprese di progettazione, il capo dell'impresa di progettazione nomina una persona o un gruppo di persone responsabile della gestione della funzione di monitoraggio della conformità di cui al punto IS.D.OR.200, lettera a), punto 12).

d) Se l'impresa condivide strutture organizzative, politiche, processi e procedure di sicurezza delle informazioni con altre imprese o con aree della propria impresa che non fanno parte dell'approvazione o della dichiarazione, il dirigente responsabile o, nel caso delle imprese di progettazione, il capo dell'impresa di progettazione può delegare le proprie attività a una persona responsabile comune.

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

e) Il dirigente responsabile o il capo dell'impresa di progettazione o la persona responsabile comune di cui alla lettera d) ha l'autorità giuridica per stabilire e mantenere le strutture organizzative, le politiche, le procedure e i processi necessari per attuare il punto IS.D.OR.200.

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

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

i) L'impresa 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.D.OR.245 Conservazione dei registri

a) L'organizzazione conserva i registri delle proprie attività di gestione della sicurezza delle informazioni.

1) L'impresa garantisce che siano archiviati e tracciabili i registri seguenti:

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

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

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

iv) i registri dei rischi individuati nella valutazione dei rischi di cui al punto IS.D.OR.205 e le relative misure di trattamento degli stessi di cui al punto IS.D.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.D.OR.215 e IS.D.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'impresa.

b) L'organizzazione conserva i registri delle qualifiche e dell'esperienza del proprio personale coinvolto nelle 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'impresa 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 registri individuali. Su richiesta, l'impresa 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'impresa.

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'impresa garantisce che i registri siano conservati utilizzando strumenti che garantiscano l'integrità, l'autenticità e l'accesso autorizzato.

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

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

1) una dichiarazione firmata dal dirigente responsabile o, nel caso delle imprese di progettazione, dal capo dell'impresa di progettazione, che confermi che l'impresa opererà sempre conformemente al presente allegato e all'ISMM. Se il dirigente responsabile o, nel caso di imprese di progettazione, il capo dell'impresa di progettazione, non è l'amministratore delegato dell'impresa, tale amministratore delegato 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 di cui al punto IS.D.OR.240, lettere b) e c);

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

4) la politica in materia di sicurezza delle informazioni dell'impresa di cui al punto IS.D.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.D.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.D.OR.200, tra cui la persona o le persone responsabili della funzione di monitoraggio della conformità di cui al punto IS.D.OR.200, lettera a), punto 12);

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

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

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

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

ii) le procedure che definiscono il modo in cui l'impresa controlla le attività appaltate di cui al punto IS.D.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'impresa. Una copia delle eventuali modifiche dell'ISMM è fornita all'autorità competente.

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

d) L'impresa 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.D.OR.255 Modifiche del sistema di gestione della sicurezza delle informazioni

a) Le modifiche dell'ISMS possono essere gestite dall'impresa e notificate all'autorità competente in una procedura sviluppata dall'impresa 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'impresa 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'impresa e le relative condizioni di approvazione a esso allegate;

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

IS.D.OR.260 Miglioramento continuo

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

b) Se si riscontrano carenze a seguito della valutazione effettuata conformemente alla lettera a), l'impresa 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'impresa riesamina inoltre gli elementi dell'ISMS interessati dalle misure adottate.