DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 30 aprile 2025

Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale. (25A02717)

(GU n.102 del 5-5-2025)

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attivita' di Governo e ordinamento della Presidenza del Consiglio dei ministri»;

Vista la legge 28 giugno 2024, n. 90, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» e, in particolare, l'art. 14 che stabilisce che con decreto del Presidente del Consiglio dei ministri siano individuati per specifiche categorie tecnologiche di beni e servizi informatici, gli elementi essenziali di cybersicurezza che taluni specifici soggetti devono tenere in considerazione nelle attivita' di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, nonche' i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialita' per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il presente decreto tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale»;

Vista la legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»;

Visto il decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante «Ulteriori misure urgenti per la crescita del Paese»;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»;

Visto il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;

Visto il decreto legislativo 3 agosto 2022, n. 123, recante «Norme di adeguamento della normativa nazionale alle disposizioni del Titolo III "Quadro di certificazione della cibersicurezza" del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la

cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013»;

Visto il decreto legislativo 4 settembre 2024, n. 138, recante «Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148»;

Visto il decreto del Presidente del Consiglio dei ministri 18 dicembre 2020, n. 179, recante «Regolamento per l'individuazione dei beni e dei rapporti di interesse nazionale nei settori di cui all'art. 4, paragrafo 1, del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, a norma dell'art. 2, comma 1-ter, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56»;

Visto il decreto del Presidente del Consiglio dei ministri 23 ottobre 2022, con il quale al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, dott. Alfredo Mantovano, e' stata delegata la firma dei decreti, degli atti e dei provvedimenti di competenza del Presidente del Consiglio dei ministri, a esclusione di quelli che richiedono una preventiva deliberazione del Consiglio dei ministri e di quelli relativi alle attribuzioni di cui all'art. 5 della legge 23 agosto 1988, n. 400;

Visto il decreto del Presidente del Consiglio dei ministri 12 novembre 2022, recante delega di funzioni in materia di cybersicurezza, con il quale l'Autorita' delegata per la sicurezza della Repubblica e' delegata a svolgere le funzioni del Presidente del Consiglio dei ministri in materia di cybersicurezza, fatte salve quelle attribuite in via esclusiva al Presidente del Consiglio dei ministri;

Visto il decreto direttoriale ACN n. 21007/2024 del 27 giugno 2024, recante «Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'art. 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221»;

Ritenuto di dover procedere alla individuazione degli elementi essenziali di cybersicurezza da tenere in considerazione nell'attivita' di approvvigionamento, per specifiche categorie tecnologiche, di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;

Tenuto conto che le specifiche categorie tecnologiche di beni e servizi informatici sono state individuate sulla base dell'utilizzo dei medesimi beni e servizi informatici nello svolgimento di funzioni essenziali per la cybersicurezza ovvero di servizi per i quali vi e' una dipendenza critica o un rischio di gravi perturbazioni delle catene di approvvigionamento;

Ritenuto, altresi', di dover procedere alla individuazione dei Paesi terzi tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, secondo un principio di gradualita' volto a tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza;

Considerati gli accordi di collaborazione vigenti fra l'Unione

europea e la NATO con Paesi terzi in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione;

Esperite valutazioni di ordine diplomatico in merito alle relazioni bilaterali con i predetti Paesi, nonche' valutazioni di ordine tecnico circa la capacita' dei fornitori di tecnologie informatiche di assicurare elevate garanzie di sicurezza nazionale sul piano operativo e funzionale;

Sulla proposta dell'Agenzia per la cybersicurezza nazionale;

Acquisito il parere del Comitato interministeriale per la sicurezza della Repubblica, nella composizione di cui all'art. 10, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

Decreta:

Art. 1

Oggetto

1. Fatto salvo quanto previsto per la tutela delle informazioni classificate, il presente decreto, ai sensi dell'art. 14, comma 1, della legge 28 giugno 2024, n. 90, individua:

a) gli elementi essenziali di cybersicurezza che i soggetti di cui all'art. 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e i soggetti privati non compresi tra quelli di cui all'art. 2, comma 2, del codice dell'amministrazione digitale e inseriti nell'elencazione di cui all'art. 1, comma 2-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, tengono in considerazione nelle attivita' di approvvigionamento di beni e servizi informatici, appartenenti a specifiche categorie tecnologiche, impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;

b) le specifiche categorie tecnologiche di beni e servizi informatici per i quali sono tenuti in considerazione gli elementi essenziali di cybersicurezza di cui alla lettera a);

c) i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialita' per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati dal presente decreto tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione;

d) i Paesi terzi di cui alla lettera c), tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Art. 2

Elementi essenziali di cybersicurezza

1. Gli elementi essenziali di cybersicurezza, di cui all'art. 14,

comma 1, della legge n. 90 del 2024, sono indicati nell'allegato 1 del presente decreto, che ne costituisce parte integrante.

Art. 3

Elenco delle categorie tecnologiche
di beni e servizi informatici

1. Le categorie di cui all'art. 1, comma 1, lettera b), sono contenute nell'elenco di cui all'allegato 2 del presente decreto, che ne costituisce parte integrante.

Art. 4

Casi in cui, per la tutela della sicurezza nazionale,
devono essere previsti criteri di premialita'

1. I casi di cui all'art. 1, comma 1, lettera c), sono quelli in cui le tecnologie di cybersicurezza sono destinate a essere impiegate dai soggetti di cui all'art. 1, comma 2-bis, del decreto-legge n. 105 del 2019, e riguardano le reti, i sistemi informativi e i servizi informatici di cui all'art. 1, comma 2, lettera b), del medesimo decreto-legge n. 105 del 2019, ovvero sono funzionali alla loro protezione fisica e logica.

2. Nei casi previsti dal comma 1, i criteri di premialita' di cui all'art. 14 della legge n. 90 del 2024, si applicano previa analisi dell'elenco di tutti i componenti di fabbricazione del prodotto o delle infrastrutture impiegate per erogare un servizio (cosiddetto B.O.M. - Bill of materials) presentato in sede di proposta o offerta dagli operatori economici. I medesimi criteri di premialita' si applicano, in maniera paritaria e uniforme, alle proposte o alle offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o dei Paesi terzi individuati nell'allegato 3 del presente decreto.

Art. 5

Elenco dei Paesi terzi

1. L'elenco dei Paesi terzi di cui all'art. 1, comma 1, lettera d), individuati in fase di prima applicazione, e' contenuto nell'allegato 3 del presente decreto, di cui costituisce parte integrante.

Art. 6

Disposizioni finali e pubblicazione

1. Il presente decreto e' soggetto ad aggiornamento periodico, anche in funzione del mutamento del contesto di riferimento, della congiuntura internazionale e dell'evoluzione tecnologica.

2. Il presente decreto e' pubblicato nella Gazzetta Ufficiale della Repubblica italiana e sara' inviato agli organi di controllo secondo le vigenti disposizioni.

Roma, 30 aprile 2025

p. Il Presidente

del Consiglio dei ministri
Il Sottosegretario di Stato
Mantovano

Allegato 1
(articolo 2)

Elementi essenziali di cybersicurezza dei beni e dei servizi informatici

Parte I. Requisiti relativi alle proprieta' dei beni e dei servizi informatici.

1) I beni e i servizi informatici sono progettati, sviluppati, prodotti e forniti in modo da garantire un livello adeguato di cybersicurezza in base ai rischi.

2) Sulla base della valutazione dei rischi di cybersicurezza, i beni e i servizi informatici:

a) sono forniti senza vulnerabilita' sfruttabili note;

b) sono forniti con una configurazione sicura per impostazione predefinita, con la possibilita' di ripristinare il bene o servizio informatico allo stato originale;

c) garantiscono che le vulnerabilita' possano essere trattate mediante aggiornamenti di sicurezza, anche, se del caso, mediante aggiornamenti di sicurezza automatici installati entro e per un periodo di tempo adeguato, abilitato come impostazione predefinita, con un meccanismo di disattivazione chiaro e di facile utilizzo, attraverso la notifica agli utilizzatori degli aggiornamenti disponibili e la possibilita' di rinviarli temporaneamente;

d) garantiscono la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo, tra cui, e in ogni caso, sistemi di autenticazione e di gestione dell'identita' o dell'accesso, e che segnalano eventuali accessi non autorizzati;

e) proteggono la riservatezza dei dati, personali o di altro tipo, conservati, trasmessi o altrimenti trattati, mediante l'uso di tecnologie allo stato dell'arte, tra cui sistemi per la cifratura dei pertinenti dati a riposo o in transito;

f) proteggono l'integrita' dei dati, personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni;

g) trattano solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione alla finalita' prevista («minimizzazione dei dati»);

h) proteggono la disponibilita' delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di mitigazione contro gli attacchi di negazione del servizio (denial of service);

i) riducono al minimo il loro impatto negativo sulla disponibilita' dei servizi forniti da altri dispositivi o reti;

l) sono progettati, sviluppati, prodotti e forniti per limitare le superfici di attacco, comprese le interfacce esterne;

m) sono progettati, sviluppati, prodotti e forniti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di mitigazione adeguati;

n) forniscono informazioni sulla sicurezza registrando e monitorando le attivita' interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi, con un meccanismo di disattivazione per l'utilizzatore;

o) offrono agli utenti la possibilita' di rimuovere in modo sicuro e agevole, su base permanente, tutti i dati e tutte le impostazioni e, qualora tali dati possano essere trasferiti ad altri beni e servizi informatici, garantiscono che cio' avvenga in modo sicuro.

Parte II. Requisiti di gestione delle vulnerabilita'.

1. La fornitura di beni e servizi informatici deve prevedere:

a) l'identificazione e la documentazione delle vulnerabilita' e dei componenti contenuti nel bene o servizio informatico, e la redazione di una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del bene o servizio;

b) in relazione ai rischi posti dai beni e servizi informatici, l'indirizzamento e la correzione tempestiva delle vulnerabilita', anche fornendo aggiornamenti di sicurezza; ove tecnicamente fattibile, nuovi aggiornamenti di sicurezza sono forniti separatamente dagli aggiornamenti della funzionalita';

c) l'esecuzione di test e riesami efficaci e periodici della sicurezza dei beni e servizi informatici;

d) una volta reso disponibile un aggiornamento di sicurezza, la condivisione e divulgazione agli utilizzatori delle informazioni sulle vulnerabilita' risolte, comprendenti una descrizione delle vulnerabilita', informazioni che consentano agli utilizzatori di identificare il bene o servizio informatico interessato, l'impatto delle vulnerabilita', la loro gravita' e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilita'; in casi debitamente giustificati, qualora ritenuto che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, e' possibile ritardare la divulgazione di informazioni su una vulnerabilita' risolta fino a quando gli utilizzatori non abbiano avuto la possibilita' di applicare la pertinente patch, in coerenza con quanto previsto dall'art. 16 del decreto legislativo 4 settembre 2024, n. 138;

e) l'adozione di misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilita' del bene o servizio informatico e dei componenti di terzi ivi contenuti, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilita' individuate;

f) l'adozione di meccanismi per distribuire in modo sicuro gli aggiornamenti dei beni e servizi informatici al fine di garantire che le vulnerabilita' siano corrette o mitigate in modo tempestivo e, ove applicabile per gli aggiornamenti di sicurezza, in modo automatico;

g) l'identificazione dei fornitori e dei partner terzi di sistemi informatici, componenti e servizi, la loro prioritizzazione e valutazione, utilizzando, allo scopo, un processo di valutazione del rischio inerente alla catena di approvvigionamento cyber;

h) l'adozione di meccanismi per garantire che, qualora disponibili, siano diffusi tempestivamente e gratuitamente, aggiornamenti di sicurezza al fine di risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che

forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare.

Allegato 2
(articolo 3)

Elenco delle categorie tecnologiche di beni e servizi informatici per le quali sono necessari elementi essenziali di cybersicurezza

Parte di provvedimento in formato grafico

Allegato 3
(articolo 5)

Elenco alfabetico dei Paesi terzi tra quelli che sono parte di accordi di collaborazione sia con l'Unione europea sia con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione

1. Australia
2. Corea del Sud
3. Giappone
4. Israele
5. Nuova Zelanda
6. Svizzera