

DECRETI PRESIDENZIALI

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.

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività 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 attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità 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 cybersicurezza" 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 cybersicurezza, e alla certificazione della cybersicurezza 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 cybersicurezza 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, è 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'Autorità delegata per la sicurezza della Repubblica è 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'attività 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 è una dipendenza critica o un rischio di gravi perturbazioni delle catene di approvvigionamento;

Ritenuto, altresì, 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 gradualità 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;

Esperate valutazioni di ordine diplomatico in merito alle relazioni bilaterali con i predetti Paesi, nonché valutazioni di ordine tecnico circa la capacità 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 attività 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 premialità 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 premialità

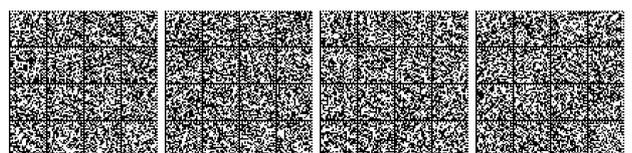
1. I casi di cui all'art. 1, comma 1, lettera *c)*, sono quelli in cui le tecnologie di cybersicurezza sono destinate a essere impiegate dai soggetti di cui all'art. 1, comma 2-bis, del decreto-legge n. 105 del 2019, e riguardano le reti, i sistemi informativi e i servizi informatici di cui all'art. 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 premialità 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 premialità 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, è contenuto nell'allegato 3 del presente decreto, di cui costituisce parte integrante.



Art. 6.

Disposizioni finali e pubblicazione

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

2. Il presente decreto è pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana e sarà 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 proprietà 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 vulnerabilità sfruttabili note;

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

c) garantiscono che le vulnerabilità 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 possibilità 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'identità 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'integrità 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 finalità prevista («minimizzazione dei dati»);

h) proteggono la disponibilità 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 disponibilità 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 attività 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 possibilità 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 ciò avvenga in modo sicuro.

Parte II. Requisiti di gestione delle vulnerabilità.

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

a) l'identificazione e la documentazione delle vulnerabilità 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 vulnerabilità, anche fornendo aggiornamenti di sicurezza; ove tecnicamente fattibile, nuovi aggiornamenti di sicurezza sono forniti separatamente dagli aggiornamenti della funzionalità;

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 vulnerabilità risolte, comprendenti una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il bene o servizio informatico interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritenuto che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, è possibile ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità 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 vulnerabilità del bene o servizio informatico e dei componenti di terzi ivi contenuti, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate;

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

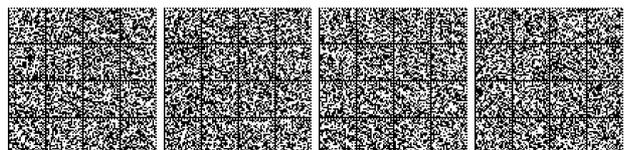
g) l'identificazione dei fornitori e dei *partner* terzi di sistemi informatici, componenti e servizi, la loro prioritizzazione e valutazione, utilizzando, allo scopo, un processo di valutazione del rischio inerente alla catena di approvvigionamento *cyber*;

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.

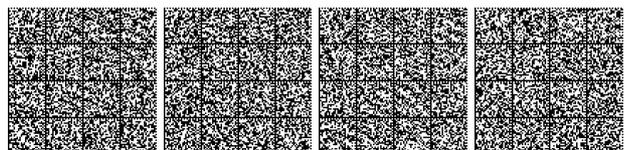


Elenco delle categorie tecnologiche di beni e servizi informatici
per le quali sono necessari elementi essenziali di cybersicurezza

Elenco tassativo delle categorie di cui all'articolo 3	Elenco non tassativo dei codici CPV (<i>Common Procurement Vocabulary</i>)
1. Sistemi di gestione dell'identità e <i>software</i> e <i>hardware</i> per la gestione degli accessi privilegiati, compresi i lettori di autenticazione e controllo degli accessi, tra cui i lettori biometrici	30233300-4 Lettori di <i>smart card</i> 30233310-7 Lettori di impronte digitali 30233320-0 Lettori combinati di <i>smart card</i> e di impronte digitali 48730000-4 Pacchetti <i>software</i> di sicurezza 48731000-1 Pacchetti <i>software</i> di sicurezza dei file 48732000-8 Pacchetti <i>software</i> di sicurezza dei dati
2. <i>Software</i> che cercano, rimuovono o mettono in quarantena i <i>software</i> maligni	48731000-1 Pacchetti <i>software</i> di sicurezza dei file 48732000-8 Pacchetti <i>software</i> di sicurezza dei dati 48760000-3 Pacchetti <i>software</i> di protezione dai virus 48761000-0 Pacchetti <i>software</i> antivirus
3. Prodotti con elementi digitali con funzione di rete privata virtuale (VPN)	48200000-0 Pacchetti <i>software</i> per reti, Internet e intranet 48211000-0 Pacchetti <i>software</i> per l'interconnettività di piattaforme 48220000-6 Pacchetti <i>software</i> per Internet e intranet 48510000-6 Pacchetti <i>software</i> di comunicazione 48730000-4 Pacchetti <i>software</i> di sicurezza 48821000-9 <i>Server</i> di rete 48517000-5 Pacchetti <i>software</i> IT 48219100-7 Pacchetti <i>software</i> gateway



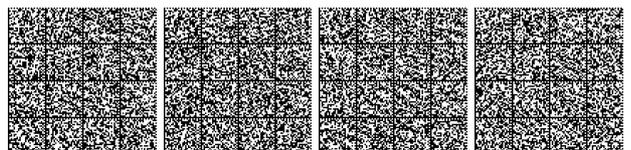
4. Sistemi di gestione della rete	<p>48517000-5 Pacchetti <i>software</i> IT</p> <p>48219000-6 Pacchetti <i>software</i> vari per reti</p> <p>48210000-3 Pacchetti <i>software</i> per reti</p> <p>48200000-0 Pacchetti <i>software</i> per reti, Internet e intranet</p> <p>48219500-1 Pacchetti <i>software</i> per <i>switch</i> o <i>router</i></p> <p>48219700-3 Pacchetti <i>software</i> per <i>server</i> di comunicazione</p> <p>48781000-6 Pacchetti <i>software</i> di gestione di sistemi</p> <p>48151000-1 Sistema di controllo informatico</p>
5. Sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)	<p>48517000-5 Pacchetti <i>software</i> IT</p> <p>48730000-4 Pacchetti <i>software</i> di sicurezza</p>
6. Infrastrutture a chiave pubblica e <i>software</i> per il rilascio di certificati digitali	<p>48730000-4 Pacchetti <i>software</i> di sicurezza</p> <p>48732000-8 Pacchetti <i>software</i> di sicurezza dei dati</p> <p>48800000-6 Sistemi e <i>server</i> di informazione</p> <p>48810000-9 Sistemi di informazione</p> <p>48151000-1 Sistema di controllo informatico</p>
7. <i>Router</i> , modem, anche di tipo satellitare, per la connessione a internet e <i>switch</i>	<p>30200000-1 Apparecchiature informatiche e forniture</p> <p>32400000-7 <i>Network</i></p> <p>32410000-0 Rete locale</p> <p>32412000-4 Rete di comunicazioni</p> <p>32412100-5 Rete di telecomunicazioni</p> <p>32412120-1 Intranet</p> <p>32415000-5 Rete <i>Ethernet</i></p> <p>32420000-3 Apparecchiature di rete</p> <p>32422000-7 Componenti di rete</p> <p>32424000-1 Infrastruttura di rete</p> <p>32427000-2 Sistema di rete</p> <p>32552410-4 Modem</p>



	32413100-2 <i>Router</i> di rete 32500000-8 Materiali per telecomunicazioni 32260000-3 Apparecchiature per la trasmissione di dati
8. Microprocessori con funzionalità legate alla sicurezza	31712116-6 Microprocessori 31712200-2 Microsistemi
9. Microcontrollori con funzionalità legate alla sicurezza	31712116-6 Microprocessori 31712200-2 Microsistemi
10. Circuiti integrati per applicazioni specifiche (ASIC), sistemi integrati su singolo chip (SOC) e reti di porte programmabili dall'utilizzatore (FPGA) con funzionalità legate alla sicurezza	31712116-6 Microprocessori 31712200-2 Microsistemi
11. <i>Firewall</i> , sistemi di rilevamento e prevenzione delle intrusioni	31712110-4 Circuiti elettronici integrati e microassemblaggi 31712113-5 Schede a circuiti integrati 31712114-2 Circuiti elettronici integrati 31712117-3 Pacchetti di circuiti integrati
12. Dispositivi <i>hardware</i> con cassette di sicurezza	30210000-4 Macchine per l'elaborazione di dati (<i>hardware</i>) 30211300-4 Piattaforme informatiche
13. <i>Gateway</i> per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23, della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, e altri dispositivi a fini di sicurezza avanzati, compreso il trattamento crittografico sicuro;	38800000-3 Attrezzature di controllo dei processi industriali e attrezzature di controllo a distanza 38820000-9 Attrezzatura per controllo a distanza
14. Carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri	30162000-2 Carte intelligenti
15. Sistemi di storage di rete (<i>Network Attached Storage, Storage Area Network</i>)	32400000-7 <i>Network</i> 30234500-3 Strumenti di stoccaggio di memoria 30233000-1 Dispositivi di stoccaggio e lettura di dati



16. Sistemi e servizi di <i>back-up</i>	48710000-8 Pacchetti <i>software</i> di <i>back-up</i> o recupero 72910000-2 Servizi di <i>back-up</i> informatico
17. Sistemi di videosorveglianza per controllo accessi e sicurezza fisica, nonché sistemi di acquisizione immagini per finalità di controllo, compresi gli scanner	32323500-8 Sistema di videosorveglianza 38582000-8 / 38581000-1 Scanner per controllo bagagli e merci
18. Servizi di consulenza, sviluppo e manutenzione di piattaforme <i>software</i> afferenti alle categorie 1, 2, 3, 4, 5, 6, 11, 15, 16 e 17	72200000-7 Programmazione di <i>software</i> e servizi di consulenza 72230000-6 Servizi di sviluppo di <i>software</i> personalizzati 72210000-0 Servizi di programmazione di prodotti <i>software</i> in pacchetti 72240000-9 Servizi di analisi e programmazione di sistemi 72260000-5 Servizi connessi al <i>software</i> 72530000-9 Servizi per rete informatica 72550000-5 Servizi di audit informatico 72570000-1 Servizi di <i>back-up</i> informatico 72250000-2 Servizi di manutenzione e assistenza sistemi.
19. Servizi <i>cloud</i>	72300000-8 Servizi di elaborazione dati 72310000-1 Servizi di trattamento dati 72400000-4 Servizi di Internet 72410000-7 Servizi di <i>provider</i> 72416000-9 Fornitori di servizi di applicazioni 72500000-0 Servizi informatici
20. Sistemi di sicurezza gestiti (<i>Managed Security Services – MSS</i>)	72300000-8 Servizi di elaborazione dati 72314000-9 Servizi di raccolta e di collazione dati 72315000-6 Servizi di gestione e supporto di reti di trasmissione dati 72315100-7 Servizi di assistenza per una rete di trasmissione dati



	72315200-8 Servizi di gestione di reti di trasmissione dati 72316000-3 Servizi analisi di dati
21. Componenti <i>hardware</i> e <i>software</i> per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali	42961200-2 Sistemi SCADA (<i>Supervisory Control And Data Acquisition</i>)
22. <i>Software</i> di controllo droni	34711200-6 Aeromobili senza pilota

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

25A02717

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'AGRICOLTURA, DELLA SOVRANITÀ ALIMENTARE E DELLE FORESTE

DECRETO 19 marzo 2025.

Rettifica dell'articolo 8 dell'Avviso pubblico a presentare proposte - produzioni vegetali, campagna assicurativa 2024 - approvato con decreto 7 febbraio 2025, n. 57047. Piano strategico nazionale della PAC 2023-2027 - Intervento SRF.01.

IL DIRETTORE GENERALE
DELLO SVILUPPO RURALE

Visto il regolamento (UE) 2021/2115 del Parlamento europeo e del Consiglio del 2 dicembre 2021, recante norme sul sostegno ai piani strategici che gli Stati membri devono redigere nell'ambito della politica agricola comune (piani strategici della PAC) e finanziati dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR) e che abroga i regolamenti (UE) n. 1305/2013 e (UE) n. 1307/2013;

Visto il regolamento (UE) n. 2021/2116 del Parlamento europeo e del Consiglio del 2 dicembre 2021 sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune e che abroga il regolamento (UE) n. 1306/2013;

Visto il piano strategico nazionale della PAC (PSP) 2023-2027 approvato dalla Commissione europea con decisione C(2022) 8645 del 2 dicembre 2022, così come modificato da ultimo con decisione C(2024) 8662 dell'11 dicembre 2024, che ricomprende gli interventi di cui all'art. 76 del regolamento (UE) n. 2115/2021 inerenti alla gestione del rischio;

Visto il decreto ministeriale 22 marzo 2024, n. 138401 recante approvazione del Piano di gestione dei rischi in agricoltura 2024 (PGRA 2024) pubblicato nella *Gazzetta ufficiale* della Repubblica italiana n. 112 del 15 maggio 2024;

Visto il decreto direttoriale 30 maggio 2024, n. 242149 di modifica al PGRA 2024 per il differimento dei termini di sottoscrizione delle polizze assicurative e coperture mutualistiche a copertura dei rischi sulle colture permanenti, pubblicato nella *Gazzetta ufficiale* della Repubblica italiana n. 157 del 6 luglio 2024;

