DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 4 giugno 2025, n. **111**.

Regolamento recante modificazioni all'allegato A al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81.

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»;

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» e, in particolare, l'articolo 1, commi 3 e 4-*bis*;

Visto il decreto legislativo 30 luglio 1999, n. 300, recante: «Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59»;

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 del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante: «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza»;

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, dottor 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'articolo 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;

Considerato che le attività di accesso alle reti, ai sistemi informativi e ai servizi informatici (beni ICT) non autorizzate o con abuso dei privilegi concessi, ivi compreso il caso in cui non siano pertinenti al corretto svolgimento delle mansioni di chi effettua l'accesso, costituiscono un utilizzo improprio dei medesimi beni ICT, in considerazione del pregiudizio derivante dalla perdita della riservatezza dei dati e delle informazioni trattate attraverso i predetti beni e, quindi, concretizzano un incidente ai sensi dell'articolo 1, comma 1, lettera *h)*, del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 81 del 2021;

Considerato, pertanto, che occorre prevedere una specifica categoria di incidenti relativi ad un utilizzo improprio aventi impatto sui beni ICT e che gli stessi incidenti siano oggetto di notifica ai sensi dell'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 81 del 2021;

Ritenuto, pertanto, di aggiornare la tabella 1 di cui all'Allegato A al decreto del Presidente del Consiglio dei ministri n. 81 del 2021, con la predetta specifica di natura meramente tecnica;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi, nell'adunanza dell'11 marzo 2025;

Acquisiti i pareri delle Commissioni parlamentari competenti per materia della Camera dei deputati e del Senato della Repubblica;

Sulla proposta del Comitato interministeriale per la cybersicurezza;

ADOTTA
il seguente regolamento:

Art. 1.

Modificazioni all'Allegato A al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81

1. All'Allegato A al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, la tabella 1 è sostituita dalla tabella allegata al presente regolamento.

2. All'attuazione delle disposizioni di cui al presente decreto si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il presente decreto munito del sigillo dello Stato sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 4 giugno 2025

p. Il Presidente
del Consiglio dei ministri
Il Sottosegretario di Stato
alla Presidenza del Consiglio dei ministri
MANTOVANO

Visto, *il Guardasigilli:* NORDIO

Registrato alla Corte dei conti il 24 luglio 2025
Ufficio di controllo sugli atti della Presidenza del Consiglio dei ministri, del Ministero della giustizia e del Ministero degli affari esteri e della cooperazione internazionale, n. 1968

ALLEGATO

«TABELLA 1

Identificativo (incidente con impatto ICP)	**Categoria**	**Descrizione**
ICP-A-1	**Infezione (*Initial exploitation*)**	**Infezione (Initial exploitation)**. Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o malware veicolato attraverso vettori di infezione o sfruttando vulnerabilità di risorse esposte in rete.
ICP-A-2	**Guasto (*Fault*)**	Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, in termini di risorse di calcolo, memoria e/o banda passante.
ICP-A-3		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, di *hot-replica* e/o *cold-replica* e/o sito(i) di *disaster recovery*, se previsti.
ICP-A-4		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, in termini di indisponibilità, di perdita irreversibile o di corruzione irreversibile dei dati provenienti dalle componenti di campo (attuatori e sensori).
ICP-A-5		Dati *hot-replica* e/o *cold-replica* e/o sito(i) di *disaster recovery* e/o *backup*, se previsti, persi o corrotti in modo irreversibile.
ICP-A-6		Perdita di confidenzialità o integrità.
ICP-A-7		Perdita e/o corruzione dati irreversibile.
ICP-A-8		Perdita e/o compromissione di chiavi di cifratura e/o certificati.
ICP-A-9		Perdita e/o compromissione di credenziali utenti.
ICP-A-10		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto dalle misure di sicurezza di cui all'allegato B, in termini di impossibilità di accesso fisico alle componenti.

Identificativo (incidente con impatto ICP)	**Categoria**	**Descrizione**
ICP-A-11	**Installazione (*Establish Persistence*)**	**Ottenimento di privilegi di livello superiore (*Privilege Escalation*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore.
ICP-A-12		**Persistenza (*Persistence*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere persistenza di codice malevolo o d'accesso.
ICP-A-13		**Evasione delle difese (*Defence Evasion*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche attraverso cui sono stati effettivamente elusi i sistemi di sicurezza.
ICP-A-14		**Comando e Controllo (*Command and Control*).** Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.
ICP-A-15	**Movimenti laterali (*Lateral Movement*)**	**Esplorazione (*Discovery*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione.
ICP-A-16		**Raccolta di credenziali (*Credential Access*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate.
ICP-A-17		**Movimenti laterali (*Lateral Movement*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad accedere o eseguire codice tra risorse interne della rete.
ICP-A-18	**Azioni sugli obiettivi (*Action on objs*)**	**Raccolta (*Collection*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a raccogliere, dall'interno della rete, dati di interesse di terze parti o ne rinviene copie non autorizzate.
ICP-A-19		**Esfiltrazione (*Exfiltration*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne.
ICP-A-20		**Accesso non autorizzato o con abuso dei privilegi concessi**. Il soggetto ha evidenza, anche sulla base di parametri quali-quantitativi, dell'accesso non autorizzato o con abuso dei privilegi concessi, dall'interno della rete, a dati digitali.

».

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'Amministrazione competente per materia, ai sensi dell'art. 10, commi 2 e 3 del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con D.P.R. 28 dicembre 1985, n. 1092, al solo fine di facilitare la lettura delle disposizioni di legge modificate e alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

Note alle premesse:

— La legge 23 agosto 1988, n. 400 recante: «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri», è pubblicata nella *Gazzetta Ufficiale* n. 214 del 12 settembre 1988.

— Si riporta il testo dell'art. 1 del decreto-legge 21 settembre 2019, n. 105 recante: «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica», pubblicato nella *Gazzetta Ufficiale* n. 222 del 21 settembre 2019, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica.

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC):

a) sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell'individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;

2-*bis*) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale.

2-*bis*. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera *a)*, è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC, entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2. Il predetto atto amministrativo, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità di cui al presente comma.

2-*ter*. Gli elenchi dei soggetti di cui alla lettera *a)* del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge 3 agosto 2007, n. 124.

3. Entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative, adottato su proposta del CIC:

a) sono definite le procedure secondo cui i soggetti di cui al comma 2-*bis* notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera *b)*, al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) Italia, che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea relative:

1) alla struttura organizzativa preposta alla gestione della sicurezza;

1-*bis*) alle politiche di sicurezza e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

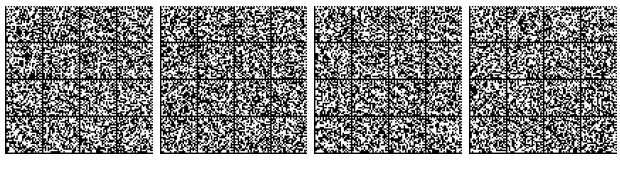
6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti 7.

3-*bis*.

4. All'elaborazione delle misure di cui al comma 3, lettera *b)*, provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.



4-*bis*. Gli schemi dei decreti di cui ai commi 2 e 3 sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il decreto può essere comunque adottato. I medesimi schemi sono altresì trasmessi al Comitato parlamentare per la sicurezza della Repubblica.

4-*ter*. L'atto amministrativo di cui al comma 2-*bis* e i suoi aggiornamenti sono trasmessi, entro dieci giorni dall'adozione, al Comitato parlamentare per la sicurezza della Repubblica.

5. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalità di cui ai commi 2, 3, 4 e 4-*bis* con cadenza almeno biennale.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, sono disciplinati le procedure, le modalità e i termini con cui:

a) i soggetti di cui al comma 2-*bis*, che intendano procedere, anche per il tramite delle centrali di committenza alle quali essi sono tenuti a fare ricorso ai sensi dell'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operatività del CVCN e comunque dal 30 giugno 2022. Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con i soggetti di cui al comma 2-*bis*, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di hardware e software, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni. Decorso il termine di cui al precedente periodo, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In relazione alla specificità delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, individuati ai sensi del comma 2, lettera *b)*, i predetti Ministeri, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal presente decreto, possono procedere, con le medesime modalità e i medesimi termini previsti dai periodi precedenti, attraverso la comunicazione ai propri Centri di valutazione accreditati per le attività di cui al presente decreto, ai sensi del comma 7, lettera *b)*, che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi i predetti Centri informano il CVCN con le modalità stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera *b)*.

Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera *b)*, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati;

b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera *b)*, assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa, di cui alla lettera *a)* del presente comma, la propria collaborazione per l'effettuazione delle attività di test di cui alla lettera *a)* del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì alla Presidenza del Consiglio dei ministri le analoghe segnalazioni dei Centri di valutazione dei Ministeri dell'interno e della difesa, di cui alla lettera *a)*;

c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera *b)*, dal comma 3, dal presente comma e dal comma 7, lettera *b)*, impartendo, se necessario, specifiche prescrizioni; nello svolgimento delle predette attività di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi è effettuato in conformità a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera *b)*, connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.

7. Nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza di cui al comma 3, lettera *b)*, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;

b) ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attività di cui al comma 6, lettera *a)*, dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del CIC, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni. Con lo stesso decreto sono altresì stabiliti i raccordi, ivi compresi i contenuti, le modalità e i termini delle comunicazioni, tra il CVCN e i predetti laboratori, nonché tra il medesimo CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa, di cui al comma 6, lettera *a)*, anche la fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesimi condizioni e livelli di rischio;

c) elabora e adotta, previo conforme avviso del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

8. La notifica d'incidente ai sensi del comma 3, lettera *a)*, effettuata dai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che rientrano nell'ambito di applicazione del decreto legislativo

di recepimento della direttiva (UE) 2022/2555 assolve agli obblighi in materia di notifica di incidente di cui all'articolo 25 del decreto legislativo medesimo.

8-*bis*. Ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che non sono individuati come soggetti essenziali o importanti ai sensi degli articoli 3 e 6 del decreto legislativo di recepimento della direttiva (UE) 2022/2555, si applicano gli obblighi di cui al capo IV e le attività ispettive e sanzionatorie di cui al capo V previste per i soggetti essenziali ai sensi del medesimo decreto legislativo, limitatamente ai sistemi informativi e di rete diversi da quelli inseriti nell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del presente decreto. L'Agenzia per la cybersicurezza nazionale, sentito il tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, stabilisce con propria determina termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al presente comma.

9. Salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione, di aggiornamento e di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera *a)*, nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza di cui al comma 3, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

d) la mancata comunicazione di cui al comma 6, lettera *a)*, nei termini prescritti, è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN ovvero dai Centri di valutazione di cui al comma 6, lettera *a)*, è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

f) la mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera *a)*, da parte dei soggetti di cui al medesimo comma 6, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

g) il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica svolte ai sensi del comma 6, lettera *c)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

h) il mancato rispetto delle prescrizioni di cui al comma 7, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

10. L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in assenza della comunicazione o del superamento dei test o in violazione delle condizioni di cui al comma 6, lettera *a)*, comporta, oltre alle sanzioni di cui al comma 9, lettere *d)* ed *e)*, l'applicazione della sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.

11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera *b)*, o al comma 6, lettera *a)*, o delle attività ispettive e di vigilanza previste dal comma 6, lettera *c)*, fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera *b)*, o ai fini delle comunicazioni di cui al comma 6, lettera *a)*, o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera *c)* od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni.

11-*bis*. All'articolo 24-*bis*, comma 3, del decreto legislativo 8 giugno 2001, n. 231, dopo le parole: "di altro ente pubblico," sono inserite le seguenti: "e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105,".

12. Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei ministri, per i soggetti pubblici e per i soggetti di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma.

13. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 9, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

14. Per i dipendenti dei soggetti pubblici di cui al comma 2-*bis*, la violazione delle disposizioni di cui al presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile.

15. Le autorità titolari delle attribuzioni di cui al presente decreto assicurano gli opportuni raccordi con il Dipartimento delle informazioni per la sicurezza e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

16. La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni di cui al presente decreto può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

17.

18. Gli eventuali adeguamenti alle prescrizioni di sicurezza definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2-*bis*, sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

19. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione del Ministero dell'interno, di cui ai commi 6 e 7, è autorizzata la spesa di euro 200.000 per l'anno 2019 e di euro 1.500.000 per ciascuno degli anni 2020 e 2021.

19-*bis*. Il Presidente del Consiglio dei ministri coordina la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte.

19-*ter*. Nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal presente articolo è acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti dal presente articolo sono sospesi per un periodo di quarantacinque giorni.».

— Il decreto legislativo 30 luglio 1999, n. 300 recante: «Riforma dell'organizzazione del Governo, a norma dell'art. 11 della legge 15 marzo 1997, n. 59», è pubblicato nella *Gazzetta Ufficiale* n. 203 del 30 agosto 1999.

— Il decreto-legge 14 giugno 2021, n. 82 recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», pubblicato nella *Gazzetta Ufficiale* n. 140 del 14 giugno 2021 è convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

Note all'art. 1:

— Il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante: «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza», è pubblicato nella *Gazzetta Ufficiale* n. 138 del 11 giugno 2021.

25G00116