MISSIONE 1 – IL PIANO NAZIONALE RIPRESA E RESILIENZA (PNRR) E LA CYBERSICUREZZA - Soggetti, infrastrutture, definizione e disciplina del perimetro di sicurezza nazionale cibernetica (*Appendice I*)

PNRR

Dossier

Sommario

1.1. Il perimetro di sicurezza nazionale cibernetica

L'art. 1 del D.L. 21 settembre 2019, n. 105 *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 istituisce il c.d. *perimetro di sicurezza nazionale cibernetica* quale strumento teso ad assicurare *un livello elevato di sicurezza* di reti, sistemi informativi e servizi informatici dei soggetti pubblici e privati[1] da cui dipende:

- l'esercizio di una funzione essenziale dello Stato[2];
- 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[3].

L'istituzione di un *perimetro di sicurezza nazionale cibernetica*, grazie anche agli oneri cui sono sottoposti i soggetti che ne fanno parte (cfr. *infra*) costituisce un tassello fondamentale nello sviluppo e nel consolidamento dell'*architettura italiana di cyber security*.

Il secondo comma dell'art. 1 affida ad un decreto del Presidente del Consiglio dei ministri:

a) la definizione di modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica. L'elencazione di tali soggetti è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, non soggetto a pubblicazione, per il quale è escluso il diritto di accesso;

---

[1] In particolare rientrano nel *perimetro di sicurezza nazionale cibernetica* le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati aventi una sede nel territorio nazionale, individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici – interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – dalle Amministrazioni competenti nei rispettivi settori.

[2] Si tratta di tutti i soggetti a cui l'ordinamento attribuisce compiti rivolti ad assicurare la continuità dell'azione di governo e degli organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionale, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario, e dei trasporti.

[3] Rientrano in quest'ambito i soggetti che realizzano:
- attività strumentali all'esercizio di funzioni essenziali dello Stato;
- attività necessarie per l'esercizio e il godimento dei diritti fondamentali;
- attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;
- attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale.

b) la definizione dei criteri con i quali i soggetti preposti predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica[4];

La delega regolamentare in questione ha trovato attuazione con l'emanazione del D.P.C.M.30 luglio 2020, n. 131 *Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*.

1.2 L'individuazione delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica

Gli artt. 2 e 3 del D.P.C.M. n. 131/2020, individuano i criteri soggettivi ed oggettivi per l'individuazione degli attori che esercitano funzioni essenziali e/o che prestano servizi essenziali.

Dal punto di vista soggettivo è considerato *esercente una funzione essenziale dello Stato* il soggetto a cui l'ordinamento attribuisce compiti rivolti ad assicurare:

- la continuità dell'azione di Governo e degli Organi costituzionali;
- la sicurezza interna ed esterna;
- la difesa dello Stato;
- le relazioni internazionali;
- la sicurezza e l'ordine pubblico;
- l'amministrazione della giustizia;
- la funzionalità dei sistemi economico e finanziario e dei trasporti.

[4] All'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica* istituito, a supporto del CISR tecnico (organismo tecnico di supporto al *Comitato interministeriale per la sicurezza della Repubblica*) di cui all'art. 6 del Regolamento di cui al D.P.C.M. 30 luglio 2020, n. 131 (cfr. *infra*).

Riguardo alla prestazione di servizi essenziali, sempre sotto il profilo soggettivo, la norma (art. 2, comma 1, lett. b)) chiarisce che un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato laddove ponga in essere:

- attività strumentali all'esercizio di funzioni essenziali dello Stato;
- attività necessarie per l'esercizio e il godimento dei diritti fondamentali;
- attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;
- attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Il secondo comma dell'art. 2 al fine di contemperare l'autonomia degli Organi costituzionali con le oggettive esigenze di sicurezza dispone che tali organi, ove intendano adottare, per le proprie reti e i propri sistemi informativi e servizi informatici, misure di sicurezza analoghe a quelle previste dal D.L. n. 105/2019, possono concludere per tali finalità appositi accordi con il Presidente del Consiglio dei ministri.

Sotto il profilo oggettivo del settore di attività, ai fini dell'inclusione nel perimetro, l'art. 3 del D.P.C.M. n. 131/2020 chiarisce che sono oggetto di individuazione, in applicazione del criterio di gradualità, i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni del *Comitato interministeriale per la sicurezza della Repubblica*, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo:

a) interno;

b) difesa;

c) spazio e aerospazio;

d) energia;

e) telecomunicazioni;

f) economia e finanza;

g) trasporti;

h) servizi digitali;

i) tecnologie critiche, di cui all'articolo 4, paragrafo 1, lettera b), del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo;

l) enti previdenziali/lavoro.

1.3 Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica

L'art. 6 del D.P.C.M. n. 131/2020 istituisce il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica* con funzioni di supporto al *CISR tecnico*. In particolare, il *CISR tecnico* si avvale del Tavolo interministeriale:

a) per l'esercizio delle funzioni istruttorie ai fini dell'elencazione dei soggetti inclusi nel perimetro (di cui al precedente art. 5);

b) ai fini del supporto per ogni altra attività attribuita dalla normativa vigente al *CISR* o al *CISR tecnico*.

Il *Tavolo interministeriale* si riunisce periodicamente, almeno una volta ogni 6 mesi, e può essere convocato d'iniziativa del presidente o su richiesta di almeno un componente designato, in relazione alla trattazione di specifici argomenti.

Il Tavolo interministeriale è presieduto da un vice direttore generale del *Dipartimento delle informazioni per la sicurezza presso la Presidenza del Consiglio dei ministri* (DIS), ed è composto da:

- due rappresentanti di ciascuna amministrazione CISR;
- un rappresentante per ciascuna delle due Agenzie (*CISR* o al *CISR tecnico*);

– due rappresentanti degli altri Ministeri di volta in volta interessati[5]

Possono essere chiamati a partecipare alle riunioni rappresentanti di altre pubbliche amministrazioni, nonché di enti e operatori pubblici e privati. La partecipazione alle riunioni del Tavolo interministeriale costituisce dovere d'ufficio e non sono, pertanto, dovuti gettoni di presenza, compensi, rimborsi spese o altri emolumenti comunque denominati.

1.3.1 La Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici

Ai sensi dell'art. 7, comma 2, del D.P.C.M. n. 131/2020, ricevuta la comunicazione dell'avvenuta iscrizione nell'elenco, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale[6] provvedono:

a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati *l'impatto di un incidente sul bene ICT*[7] e le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione;

b) a predisporre l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. In fase di prima applicazione e fino all'aggiornamento del D.P.C.M. n. 131/2020, ai sensi dell'art. 1, comma 5, del D.L. n. 105/2019, sono individuati, all'esito dell'analisi del rischio, in ossequio al principio di gradualità, i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate si applica quanto previsto dall'art.1, comma 2, lettera b), del D.L. n. 105/2019. Pertanto, i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici

[5] In particolare, i rappresentanti dei Ministeri interessati sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare, di cui almeno uno in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.
[6] A tal proposito si ricorda che ai sensi dell'art. 4, comma 1, lettera c) del D.P.C.M. n. 131/2020 sono considerati funzione essenziale o servizio essenziale quelli per i quali in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime.
[7] In termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali.

di rispettiva pertinenza, 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[8]. All'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica*. Entro sei mesi dalla data della comunicazione dell'avvenuta iscrizione nell'elenco, i soggetti pubblici e privati iscritti nell'elencazione contenuta nello specifico atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC e i soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata 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[9].

L'architettura e la componentistica relative ai beni ICT individuati, sono descritte conformemente al modello predisposto, sentito il CISR tecnico, dal DIS[10], che ne cura la comunicazione ai soggetti interessati unitamente alla comunicazione dell'avvenuta iscrizione nell'elenco (art. 8, D.P.C.M. n. 131/2020).

Il decreto previsto da questa norma viene aggiornato con cadenza almeno biennale.

1.3.2 Modalità di trasmissione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici

Oltre agli adempimenti testé descritti l'art. 9 del D.P.C.M. n. 131/2020 prevede che entro sei mesi dalla data della comunicazione dell'avvenuta iscrizione nell'elenco della presidenza del consiglio dei ministri, i soggetti pubblici e privati iscritti e i quelli che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata trasmettano alla *Struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione* e al *Ministero dello sviluppo economico*, gli elenchi delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza comprensivi della descrizione dell'architettura e della componentistica predisposta secondo il citato modello predisposto dal DIS, sentito il CISR tecnico. La trasmissione degli elenchi di beni ICT avviene per il tramite di una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al *Nucleo per la Sicurezza*

[8] L'elenco in questione è comprensivo, anche, della relativa architettura e componentistica delle reti, dei sistemi informativi e dei servizi informatici inseriti

[9] Il *Dipartimento delle informazioni per la sicurezza*, l'AISE e l'AISI ai fini dell'esercizio delle funzioni istituzionali e l'*organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione* accedono a tali elenchi per il tramite di una specifica piattaforma digitale costituita presso l'*Agenzia per la cybersicurezza nazionale* ai sensi dell'art. 9, comma 1, del D.P.C.M. n. 131/2020.

[10] Il modello contiene l'indicazione degli elementi utili alla descrizione dei beni ICT e delle relative dipendenze.

Cibernetica (NSC), nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente. Queste disposizioni trovano applicazione anche rispetto all'aggiornamento degli elenchi di beni ICT.

La struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e il Ministero dello sviluppo economico, per i profili di rispettiva competenza, accedono a tale piattaforma per lo svolgimento delle attività di ispezione e verifica istituzionali anche ai fini dell'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative.

In relazione alle reti, ai sistemi informativi e ai servizi informatici 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, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione accede alla piattaforma in questione, limitatamente alle informazioni necessarie, individuate dal modello definito dal DIS, per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative.

Nelle more di una revisione generale delle disposizioni in materia di sicurezza (cfr. *infra*) e fatta salva l'eventuale attribuzione di classifiche previste dalla legislazione vigente, l'elencazione dei soggetti iscritti nell'elenco e gli elenchi comprensivi della descrizione dell'architettura e della componentistica, nonché dell'analisi del rischio, sono trattati, conservati e trasmessi con modalità idonee a garantirne la sicurezza, mediante misure tecniche e organizzative adeguate.

1.4. La notifica degli incidenti

L'art. 1, comma 3, del D.L. n. 105/2019 prevede che entro dieci mesi dalla data di entrata in vigore della legge di conversione (L. 18 novembre 2019, n. 133), con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative siano definite le procedure secondo cui i soggetti iscritti nell'elenco, notificano gli incidenti[11] aventi impatto su reti, sistemi informativi e servizi informatici, al *Gruppo di intervento per la sicurezza*

[11] L'art. 1, comma 1, lett. h) del D.P.C.M. 14 aprile 2021, n. 81 definisce incidente *ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*.

informatica in caso di incidente (*Computer Security Incident Response Team* - CSIRT) italiano[12] 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, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico, da un fornitore di servizi fiduciari qualificati o da un gestore di posta elettronica certificata, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato.

Con il D.P.C.M. che disciplina le procedure per la notifica degli incidenti sono stabilite, altresì, le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, 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.

[12] Il *Computer Security Incident Response Team* (CSIRT) Italiano è un organo collegiale composto da esperti di cybersecurity, istituito con l'obiettivo di massimizzare l'efficacia della prevenzione e della risposta del Paese a incidenti da cui possano derivare danni a soggetti pubblici e/o privati. A seguito della notifica il CSIRT inoltra 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, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto un fornitore di servizi fiduciari qualificati o un gestore di posta elettronica certificata, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato.

All'elaborazione di tali misure, provvedono, secondo gli ambiti di competenza il Ministero delle Imprese del Made in Italy 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.

Tale decreto viene aggiornato con cadenza almeno biennale.

1.5. L'affidamento di forniture di beni, sistemi e servizi ICT

Il sesto comma dell'art. 1, D.L. n. 105/2019 incarica il governo dell'emanazione di un regolamento[13] con cui disciplinare le procedure, le modalità e i termini con cui:

a) i soggetti inseriti nel perimetro della cybersicurezza nazionale che intendano procedere, anche per il tramite delle centrali di committenza[14] 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, appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, ne danno comunicazione al *Centro di valutazione e certificazione nazionale* (CVCN), istituito presso il Ministero dello sviluppo economico[15]. 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*, 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

[13] Da adottarsi ai sensi dell'art. 17, comma 1, della L. 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione dello stesso D.L. n. 105/2019.
[14] L'art. 1, comma 512, della L. 28 dicembre 2015, n. 208 (*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*), al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, prevede che le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione provvedano ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di ***Consip Spa*** o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.
[15] La comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego.

all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni decorsi i quali i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento[16].

b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai *Centri di valutazione* operanti presso i Ministeri dell'interno e della difesa, la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri;

c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici, dei fornitori di servizi fiduciari qualificati e dei gestori di posta elettronica certificata e il Ministero dello sviluppo economico, per i soggetti privati svolgono attività di ispezione e verifica, impartendo, se necessario, specifiche prescrizioni[17].

1.5.1 Il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54

La delega regolamentare contenuta nel citato art. 1, comma 6 del D.L. 21 n. 105/2019, ha trovato attuazione con l'emanazione del D.P.R 5 febbraio 2021, n. 54[18] il quale definisce:

a) le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del *Centro di Valutazione e Certificazione nazionale* (CVCN) e dei *Centri di valutazione del Ministero dell'interno e del Ministero della difesa* (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel

[16] 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, detti Ministeri possono procedere attraverso la comunicazione ai propri *Centri di valutazione accreditati* che impiegano le metodologie di verifica e di test definite dal CVCN. 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 stabilite dalla normativa vigente, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati.

[17] Nello svolgimento di tali 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 (*Regolamento generale sulla protezione dei dati* GDPR), e dal *Codice in materia di protezione dei dati personali*, di cui al D.Lgs. 30 giugno 2003, n. 196. Per le reti, i sistemi informativi e i servizi informatici 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.

[18] D.P.R 5 febbraio 2021, n. 54 *Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.*

perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri previsti dalla legge;

b) i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione di cui alla lettera a);

c) le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

1.5.1.1 La Procedura di valutazione del CVCN e dei CV

I soggetti inclusi nel perimetro, prima dell'avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT ne danno comunicazione al CVCN o ai CV (art. 3, D.P.R. 5 febbraio 2021, n. 54). Tale obbligo di comunicazione permane anche nel caso in cui le procedure di affidamento siano state espletate attraverso le centrali di committenza[19]. La trasmissione è effettuata in via telematica al CVCN o ai CV per le valutazioni di rispettiva competenza. I dati contenuti nelle comunicazioni sono raccolti in archivi informatici istituiti presso le Amministrazioni nelle quali operano il CVCN e i CV.

La comunicazione, oltre ai dati identificativi del soggetto incluso nel perimetro, contiene i seguenti elementi:

a) la descrizione generale dell'oggetto della fornitura;

[19] Le centrali di committenza sono amministrazioni aggiudicatrici o enti aggiudicatori che svolgono in via permanente attività di centralizzazione delle committenze riguardanti:
- l'acquisizione di forniture o servizi destinati a stazioni appaltanti;
- l'aggiudicazione di appalti e/o la conclusione di accordi quadro per lavori, forniture o servizi destinati a stazioni appaltanti.

Esse, inoltre, svolgono attività di committenza ausiliarie, di supporto alle attività di committenza quali:
- infrastrutture tecniche tali da permettere alle stazioni appaltanti l'aggiudicazione di appalti pubblici e/o la conclusione di accordi quadro per lavori, forniture o servizi;
- supporto e consulenza su svolgimento e progettazione delle procedure di appalto;
- predisposizione e gestione delle procedure di appalto in nome e per conto della stazione appaltante interessata.

L'art. 62, comma 7, del D.Lgs. 31 marzo 2023, n. 36, precisa che esse, in relazione ai requisiti di qualificazione posseduti:
a) progettano, aggiudicano e stipulano contratti o accordi quadro per conto delle stazioni appaltanti non qualificate;
b) progettano, aggiudicano e stipulano contratti o accordi quadro per conto delle stazioni appaltanti qualificate;
c) progettano, aggiudicano e stipulano convenzioni e accordi quadro ai quali le stazioni appaltanti qualificate e non qualificate possono aderire per l'aggiudicazione di propri appalti specifici;
d) istituiscono e gestiscono sistemi dinamici di acquisizione e mercati elettronici di negoziazione;
e) eseguono i contratti per conto delle stazioni appaltanti non qualificate qualora non siano qualificate per l'esecuzione.

Il successivo art. 63, tra le altre cose, precisa che Ogni stazione appaltante o centrale di committenza può effettuare le procedure corrispondenti al livello di qualificazione posseduto e a quelli inferiori.

b) l'impiego, ovvero la destinazione d'uso dell'oggetto della fornitura nell'ambito dei beni ICT;

c) la categoria di appartenenza dell'oggetto della fornitura;

d) le informazioni e i servizi che l'oggetto della fornitura deve trattare e le relative modalità di gestione;

e) le informazioni relative all'eventuale acquisizione mediante gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.

In aggiunta a tali elementi la comunicazione include il documento di analisi del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego[20]. Le metodologie per la predisposizione del documento di analisi del rischio e per l'individuazione dei livelli di severità dei test di corretta implementazione delle funzionalità di sicurezza e di intrusione a supporto dell'analisi di vulnerabilità sono definite con specifico atto del CVCN[21].

Il CVCN o i CV svolgono, secondo le rispettive competenze, il procedimento di verifica e valutazione dell'analisi documentale contenuta nella comunicazione (art. 4, D.P.R. n. 54/2021).

Il procedimento di verifica e valutazione dell'analisi documentale si articola nelle seguenti fasi:

a) verifiche preliminari[22];

b) fase di preparazione all'esecuzione dei test;

c) esecuzione dei test di *hardware* e di *software*[23].

---

[20] Il documento contiene la descrizione dei seguenti elementi:
a) l'ambiente operativo dell'ambito di impiego specificando:
1. i componenti con i quali l'oggetto della fornitura interagisce e le configurazioni di tali componenti;
2. le eventuali misure di sicurezza esistenti di tipo fisico, tecnico, procedurale, relative al personale con indicazione delle eventuali certificazioni o verifiche eseguite;
b) i requisiti di sicurezza che caratterizzano l'impiego dell'oggetto della fornitura, espressi in termini di capacità di proteggere la disponibilità, l'integrità e la riservatezza delle informazioni e i servizi.

[21] A tal fine, il CVCN, sulla base di standard tecnici di riferimento, tiene conto dell'impatto di violazioni intenzionali o accidentali sui requisiti di sicurezza che determinano eventi di indisponibilità, malfunzionamento e compromissione della funzione essenziale o del servizio essenziale.

[22] Le attività di verifica preliminare sono svolte entro il termine di quarantacinque giorni dalla comunicazione dell'avvio delle procedure di affidamento o prima della conclusione dei contratti relativi alla fornitura di beni.
Tale termine è prorogabile una sola volta, di quindici giorni, nei casi di particolare complessità, nell'ipotesi in cui l'oggetto di valutazione:
a) sia costituito da beni, sistemi e servizi ICT integrati tra di loro;
b) sia basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate;
c) interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali.
Decorsi inutilmente tali termini, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento.

[23] 5. I test si concludono entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV. Decorso inutilmente tale termine, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire l'esecuzione del contratto.

All'esito delle verifiche e dei test, il CVCN o i CV, con apposito provvedimento, definiscono eventuali condizioni e test di *hardware* e di *software* da inserire nelle clausole del bando di gara o del contratto nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro.

Ai fini dello svolgimento dei test di cui sub c), il CVCN può avvalersi di *laboratori accreditati di prova* (LAP) e si coordina, ove previsto, con i centri di valutazione del Ministero dell'Interno e del Ministero della Difesa.

Il CVCN condivide con i CV e i LAP le metodologie per l'effettuazione dei test ai sensi della normativa tecnica emanata con specifico decreto del Presidente del Consiglio dei ministri[24]. Il CVCN, i CV e i LAP assicurano, anche con strumenti adeguati, la riservatezza di tali metodologie.

Gli atti del procedimento di verifica e valutazione sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'art. 1, comma 1, del D.L. n. 105/2019[25].

– Verifiche preliminari, individuazione di condizioni e test

Le attività di verifica preliminare, individuazione di condizioni e test si apre con la comunicazione di avvio delle procedure di affidamento, a seguito della quale il CVCN o i CV effettuano le verifiche preliminari ed eventualmente richiedono al soggetto incluso nel perimetro le informazioni necessarie per assicurare la collaborazione ai fini dell'individuazione delle condizioni per il fornitore e della tipologia di test di *hardware* e di *software* da eseguire (art. 5, D.P.R. n. 54/2021). In caso di incompletezza o incongruenza delle informazioni fornite dal soggetto incluso nel perimetro i termini di conclusione del procedimento sono sospesi, per una sola volta, fino al ricevimento delle informazioni richieste.

Il CVCN e i CV possono richiedere l'esecuzione delle seguenti tipologie di test:

a) test di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto;

b) test di intrusione a supporto dell'analisi di vulnerabilità.

[24] Adottato in attuazione dell'art. 1, comma 7, lettera b), del D.L. n. 105/2019, che fissa i criteri per l'accreditamento dei laboratori.
[25] A tal proposito appare utile ricordare che la norma richiamata (l'art. 1, comma 1, del D.L. n. 105/2019) istituisce il perimetro di sicurezza nazionale cibernetica 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.

Nel caso di imposizione di test, il fornitore è tenuto ad effettuare almeno le seguenti attività propedeutiche e indispensabili alla loro esecuzione:

a) fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza;

b) provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il fornitore o presso il soggetto del perimetro;

c) fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni;

d) fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione;

e) fornire una descrizione dei test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

Il CVCN e i CV definiscono, con apposito provvedimento, da comunicarsi al soggetto incluso nel perimetro le eventuali ulteriori condizioni, i test da eseguire ed eventuali indicazioni per il supporto da parte del fornitore ai fini dell'integrazione nei bandi di gara o nei contratti con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test.

Nei bandi di gara o nei contratti, i requisiti di sicurezza dell'oggetto di fornitura sono indicati dal soggetto incluso nel perimetro adottando se necessario le opportune cautele di riservatezza, anche nei casi in cui l'acquisizione avvenga attraverso le centrali di committenza.

Il soggetto incluso nel perimetro, successivamente all'aggiudicazione della gara o della stipula del contratto, comunica al CVCN o ai CV, in via telematica, i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto di fornitura.

– La Preparazione all'esecuzione dei test

A seguito della comunicazione dei riferimenti del fornitore il CVCN e i CV verificano, ai sensi dell'art. 6 del D.P.R. n. 54/2021, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se siano in corso valutazioni. Nel caso in cui:

a) l'oggetto sia stato sottoposto a precedenti valutazioni o sia in corso di valutazione, sono effettuate le verifiche finalizzate a evitare la duplicazione di test eventualmente già eseguiti[26];

b) l'oggetto non sia stato sottoposto a precedenti valutazioni e non sia in corso di valutazione, il CVCN o i CV, se necessario in collaborazione con il soggetto incluso nel perimetro, identificano i test da eseguire escludendo quelli precedentemente eseguiti o in corso di esecuzione.

Inoltre, nei casi *sub* b):

a) il CVCN può affidare l'esecuzione dei test ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore;

b) il CVCN e i CV invitano il fornitore a predisporre le attività preliminari all'esecuzione dei test e definiscono la sede in cui svolgere tali attività.

– L'Esecuzione dei test

Ai sensi dell'art. 7, una volta concluse le attività preliminari il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel perimetro e al fornitore. I test si concludono entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV.

Con la comunicazione di avvio dei test il CVCN o i CV specificano le modalità di collaborazione dei fornitori durante l'esecuzione delle prove[27].

Nel caso in cui si verifichi un malfunzionamento dell'oggetto di valutazione o dell'ambiente di test predisposto dal fornitore che renda impossibile o difficoltosa l'esecuzione dei test, il CVCN o i CV comunicano tempestivamente al soggetto incluso nel perimetro informando anche il fornitore, i motivi che ostano al proseguimento dei test[28].

---

[26] In tali casi sull'oggetto di valutazione non sono effettuati test nei casi in cui:
a) su tutte le funzioni di sicurezza necessarie per soddisfare i requisiti di sicurezza di interesse nella nuova valutazione siano stati eseguiti o siano in corso di esecuzione sia i test di corretta implementazione, sia i test di intrusione;
b) i test di intrusione siano stati eseguiti o siano in corso di esecuzione con riferimento a livelli di severità non inferiori a quelli selezionati per la valutazione in corso.
c) nei rimanenti casi il CVCN o i CV, se necessario in collaborazione con il soggetto incluso nel perimetro, identificano i test da eseguire escludendo quelli precedentemente eseguiti o in corso di esecuzione.

[27] I test sono eseguiti, secondo le metodologie predisposte dal CVCN, presso i laboratori del CVCN, dei CV e dei LAP. I CV e i LAP sono tenuti a non divulgare tali metodologie Se necessario, i test possono essere eseguiti da personale del CVCN, dei CV e dei LAP presso il fornitore o il soggetto incluso nel perimetro.

[28] La comunicazione viene effettuata nel rispetto dei principi in tema di Comunicazione dei motivi ostativi all'accoglimento dell'istanza di cui all'art. 10-*bis* della L. 7 agosto 1990, n. 241. Nello specifico questa norma prevede che *nei procedimenti ad istanza di parte il responsabile del procedimento o l'autorità competente, prima della formale adozione di un provvedimento*

Entro il termine di dieci giorni dalla ricezione della comunicazione, il fornitore può provvedere a risolvere il malfunzionamento. La predetta comunicazione sospende i termini per la conclusione dei test (di cui all'art. 4, comma 5, del D.P.R. n. 54/2021) che iniziano nuovamente a decorrere dalla data di soluzione del malfunzionamento verificata dal CVCN o dai CV.

In caso di eventuale mancata soluzione entro il termine, il CVCN o i CV comunicano al soggetto incluso nel perimetro e al fornitore l'impossibilità di proseguire l'esecuzione dei test e concludono il procedimento indicando la motivazione.

Il CVCN, i CV e i LAP redigono un rapporto di prova nel quale sono indicati in dettaglio l'ambiente di test, le prove eseguite ed i relativi esiti.

I LAP, eventualmente incaricati per l'esecuzione dei test, trasmettono il rapporto di prova al CVCN entro sette giorni lavorativi dalla scadenza dei termini per l'esecuzione dei test. Nel caso in cui sia stato incaricato il LAP e si verifichi un malfunzionamento dell'oggetto di valutazione o dell'ambiente di test predisposto dal fornitore, lo stesso LAP informa tempestivamente il CVCN che procede ai sensi del comma 5.

– Esito della valutazione e prescrizioni di utilizzo

Il CVCN e i CV redigono il *rapporto di valutazione* contenente l'esito dei test sulla base del rapporto di prova.

Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro sessanta giorni.

In caso di esito negativo del rapporto di valutazione, il CVCN e i CV, previa comunicazione dei motivi ostativi all'accoglimento dell'istanza, comunicano al soggetto incluso nel perimetro e al fornitore il provvedimento negativo motivato.

---

negativo, comunica tempestivamente agli istanti i motivi che ostano all'accoglimento della domanda. Entro il termine di dieci giorni dal ricevimento della comunicazione, gli istanti hanno il diritto di presentare per iscritto le loro osservazioni, eventualmente corredate da documenti. La comunicazione di cui al primo periodo sospende i termini di conclusione dei procedimenti, che ricominciano a decorrere dieci giorni dopo la presentazione delle osservazioni o, in mancanza delle stesse, dalla scadenza del termine di cui al secondo periodo. Qualora gli istanti abbiano presentato osservazioni, del loro eventuale mancato accoglimento il responsabile del procedimento o l'autorità competente sono tenuti a dare ragione nella motivazione del provvedimento finale di diniego indicando, se ve ne sono, i soli motivi ostativi ulteriori che sono conseguenza delle osservazioni. In caso di annullamento in giudizio del provvedimento così adottato, nell'esercitare nuovamente il suo potere l'amministrazione non può addurre per la prima volta motivi ostativi già emergenti dall'istruttoria del provvedimento annullato. Le disposizioni di cui al presente articolo non si applicano alle procedure concorsuali e ai procedimenti in materia previdenziale e assistenziale sorti a seguito di istanza di parte e gestiti dagli enti previdenziali. Non possono essere addotti tra i motivi che ostano all'accoglimento della domanda inadempienze o ritardi attribuibili all'amministrazione.

Nel caso di esito positivo, il CVCN può imporre al soggetto incluso nel perimetro prescrizioni per l'utilizzo dell'oggetto dell'affidamento. Tali prescrizioni possono riguardare anche il mantenimento nel tempo del livello di sicurezza nell'ambiente di esercizio.

1.5.1.2 I Casi di deroga

Ai sensi dell'art. 10 del D.P.R. n. 54/2021 e dell'art. 1, comma 6, ultimo periodo, del D.L. n. 105/2019, non sono tenute agli obblighi di comunicazione testé illustrati Autorità di pubblica sicurezza e le forze di polizia.

Ai fini della deroga alla *Comunicazione di 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 all'art. 3) è considerato indispensabile procedere in sede estera, salvo motivate esigenze connesse a specifici impieghi, per le forniture dei seguenti beni, sistemi e servizi ICT, se acquisite e utilizzate nel Paese in cui i soggetti del perimetro operano, tramite uffici, sedi o filiali all'estero:

a) realizzazione e aggiornamento di reti informatiche e di telecomunicazioni;

b) servizi di connettività;

c) servizi di gestione, assistenza e manutenzione di apparati e sistemi informatici, di rete e di telecomunicazione, erogati in presenza presso la sede estera.

L'elenco e la documentazione relativa agli affidamenti effettuati sono resi disponibili per le verifiche e le ispezioni di cui al capo IV del presente decreto.

1.5.1.3 Categorie di tipologie di beni, sistemi e servizi ICT

L'art. 13, comma 1, del D.P.R. n. 54/2021 precisa che le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate sulla base dell'esecuzione o svolgimento delle seguenti funzioni:

a) commutazione oppure protezione da intrusioni e rilevazione di minacce informatiche in una rete, ivi inclusa l'applicazione di politiche di sicurezza;

b) comando, controllo e attuazione in una rete di controllo industriale;

c) monitoraggio e controllo di configurazione di una rete di comunicazione elettronica;

d) sicurezza della rete riguardo alla disponibilità, autenticità, integrità o riservatezza dei servizi offerti o dei dati conservati, trasmessi o trattati;

e) autenticazione e allocazione delle risorse di una rete di comunicazione elettronica;

f) implementazione di un servizio informatico per mezzo della configurazione di un programma *software* esistente oppure dello sviluppo, parziale o totale, di un nuovo programma *software*, costituente la parte applicativa rilevante ai fini dell'erogazione del servizio informatico stesso.

Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate con decreto del Presidente del Consiglio dei ministri sulla base dei criteri descritti nei punti da a) a f).

1.5.1.4 Le Ispezioni e le verifiche

Il capo IV (artt. da 14 a 20) del D.P.R. n.54/2021 disciplina l'attività ispettiva[29] e di verifica[30] sull'attività dei soggetti inclusi nel perimetro della cybersicurezza.

Il citato art. 14 chiarisce che le verifiche e le ispezioni hanno lo scopo di accertare l'adempimento da parte dei soggetti inclusi nel perimetro dei seguenti obblighi:

a) predisposizione, aggiornamento e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici;

[29] L'art. 1, comma 1, lett. v) del dal D.P.R. n. 54/2019 definisce l'ispezione come l'*attività di tipo ricognitivo e valutativo che si articola nell'analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto utili ad accertare l'adempimento degli obblighi previsti dal D.L. n. 105/2019*.
[30] L'art. 1, comma 1 lett. u) del D.P.R. 5 febbraio 2021, n. 54 definisce la verifica come l'*attività di analisi e controllo documentale delle evidenze al fine di accertare l'adempimento degli obblighi previsti dal D.L. n. 105/2019*.

b) notifica al CSIRT italiano (*Computer Security Incident Response Team*) degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici nei termini e con le modalità previste dalla normativa tecnica;

c) adozione delle misure di sicurezza prescritte dalla legge e dalla normativa tecnica;

d) invio al CVCN nei termini e con le modalità previste dalla normativa tecnica della *Comunicazione di 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;

e) impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in conformità alle condizioni e con superamento dei test imposti dal CVCN;

f) collaborazione per l'effettuazione delle attività di test da parte di fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici;

g) osservanza delle prescrizioni formulate dalle autorità competenti all'esito delle attività di ispezione e verifica;

h) osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto.

Dette attività di verifica e ispezione sono svolte:

a) dalla *struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione*, per i profili di pertinenza dei soggetti pubblici inclusi nel perimetro e dei soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata.

b) dalla *struttura competente in materia di tecnologie delle comunicazioni e di sicurezza informatica del Ministero dello sviluppo economico* per i soggetti privati inclusi nel perimetro;

c) dalle *strutture specializzate* previste dalla legge (art. 1, comma 6, lettera c), del D.L. n. 105/2019), secondo le rispettive competenze, limitatamente alle reti, ai sistemi informativi, ai servizi informatici, 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, che comunicano gli esiti alla Presidenza del Consiglio dei Ministri per i profili di competenza.

Ai fini dello svolgimento delle verifiche e delle ispezioni, le autorità competenti individuano, nel rispetto dei criteri di professionalità e rotazione, il personale incaricato, nonché un responsabile del procedimento ai sensi dell'art. 6 della L. n. 241/1990[31].

Ai sensi dell'art. 16, le autorità competenti dispongono verifiche e ispezioni sulla base degli atti di programmazione adottati, nonché in caso di esigenze derivanti da notifiche di incidenti, inadempimenti rilevati degli obblighi di legge e segnalazioni provenienti da altre Autorità Pubbliche.

Le ispezioni sono svolte anche successivamente alle verifiche qualora si ritenga necessario riscontrare le evidenze acquisite, oppure qualora le predette verifiche presentino elementi tali da richiedere un approfondimento.

Il responsabile del procedimento comunica ai soggetti interessati di cui all'art. 7, comma 1, della L. n. 241/1990[32], inclusi nel perimetro, l'avvio del procedimento di verifica o di ispezione, richiedendo le informazioni e la documentazione necessaria al fine dell'espletamento delle relative attività.

I destinatari di tale comunicazione nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per lo svolgimento delle attività di verifica ed ispezione, comunicandone il nominativo al responsabile del procedimento.

I procedimenti di verifica ed ispezione, si concludono, rispettivamente:

- entro il termine di centoventi giorni dalla data della comunicazione dell'avvio del procedimento di verifica;
- entro il termine di novanta giorni dalla data della comunicazione l'avvio del procedimento di ispezione.

[31] Al momento dell'accettazione dell'incarico, il personale incaricato dichiara di non trovarsi, per quanto a sua conoscenza, in una situazione di conflitto di interessi e si impegna a segnalare ogni sopravvenuta situazione di conflitto, anche potenziale.
[32] Soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti inclusi quelli che per legge debbono intervenire nel procedimento.

All'esito delle attività di verifica e di ispezione le autorità competenti possono formulare specifiche prescrizioni a cui i soggetti inclusi nel perimetro devono attenersi. Il rispetto delle prescrizioni può essere oggetto, a sua volta, di attività di verifica e ispezione.

– L'attività di verifica

Le verifiche sono effettuate mediante analisi e controllo documentale delle evidenze e di ogni altro elemento di fatto e di diritto, al fine di accertare l'adempimento degli obblighi previsti dal decreto-legge e dai relativi decreti attuativi (art. 17). Il procedimento di verifica è avviato con la comunicazione di avvio del procedimento (cfr. *supra*). I soggetti destinatari della comunicazione rendono disponibile la documentazione richiesta ai fini delle attività di verifica, entro quindici giorni dalla ricezione della comunicazione.

Durante l'esecuzione delle attività di verifica, il responsabile del procedimento, qualora le evidenze risultino incomplete o incongruenti, può richiedere chiarimenti e integrazioni che sono resi entro dieci giorni dalla ricezione della richiesta, secondo le modalità indicate dal richiedente. Dell'attività svolta nel corso delle verifiche è redatto apposito verbale che il personale incaricato trasmette al responsabile del procedimento.

Qualora nel corso della verifica vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

– L'attività ispettiva

Le ispezioni, ai sensi dell'art. 18, possono essere svolte mediante:

a) riscontro delle evidenze eventualmente acquisite in sede di verifica, qualora le stesse presentino elementi meritevoli di approfondimento;

b) analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari.

Il personale incaricato, per lo svolgimento di tali attività, può richiedere o eventualmente acquisire direttamente tutte le evidenze ritenute utili ai fini dell'accertamento.

Le ispezioni possono essere effettuate presso le sedi utilizzate dai soggetti inclusi nel perimetro nei casi di notifiche di incidenti, inadempimenti rilevati degli obblighi di legge e segnalazioni

provenienti da altre Autorità Pubbliche. Il relativo procedimento è avviato con la *comunicazione di avvio del procedimento* (cfr. *supra*), con un preavviso non inferiore a quindici giorni. L'informativa riporta:

a) le date e i siti in cui sarà effettuata l'ispezione;

b) le persone da intervistare o i loro ruoli e responsabilità;

c) le reti, i sistemi informativi e i servizi informatici da sottoporre a ispezione;

d) i nominativi del personale incaricato;

e) eventuali altre informazioni utili ai fini dell'ispezione.

Entro cinque giorni dalla ricezione della comunicazione di avvio del procedimento ispettivo, il soggetto ricevente può proporre date alternative a quelle previste per l'ispezione, individuando un termine non superiore a dieci giorni per il differimento dell'ispezione. Qualora il soggetto proponga date alternative, l'autorità competente può:

a) accettare la proposta di modifica delle date, inviando una comunicazione almeno sette giorni prima della prima data prevista per l'ispezione;

b) proporre ulteriori date e comunicarle al soggetto inviando, anche in questo caso, una comunicazione almeno sette giorni prima della prima data prevista per l'ispezione. Tali nuove date non possono essere soggette a richieste di modifica e si intendono, quindi, confermate.

Almeno cinque giorni prima dell'ispezione prevista, il soggetto sottoposto alla stessa comunica il nominativo del referente unico per lo svolgimento delle attività di ispezione (di cui all'art. 16, comma 4, del D.P.R. n. 54/2021)

Durante l'ispezione, i soggetti inclusi nel perimetro mettono a disposizione tutte le risorse umane richieste, necessarie per agevolare le relative attività, garantendo altresì l'accesso ai locali, ai dispositivi e alle informazioni rilevanti ai fini dell'ispezione, anche se non esplicitamente e preventivamente indicati nella comunicazione di avvio del procedimento ispettivo. Qualora durante il corso dell'ispezione emergano evidenze meritevoli di approfondimento, le stesse possono essere esaminate in una fase successiva.

Dell'attività svolta nel corso dell'ispezione è redatto apposito processo verbale da parte del personale incaricato che lo sottoscrive unitamente al referente unico per lo svolgimento delle attività di ispezione a ciò incaricato. Nel caso in cui quest'ultimo si rifiuti di sottoscrivere il

verbale, il personale incaricato ne dà evidenza nel verbale. Una copia del verbale è comunque rilasciata al referente unico, e una copia è trasmessa al responsabile del procedimento.

Qualora nel corso dell'ispezione vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

– Gli esiti delle attività di verifica e di ispezione

L'autorità competente, raccolti gli esiti delle attività di verifica e di ispezione, adotta il provvedimento di conclusione del procedimento, impartendo, se necessario, specifiche prescrizioni e dandone comunicazione all'interessato. Nei casi previsti, l'autorità competente avvia il procedimento per l'applicazione delle sanzioni di previste dall'articolo 1, comma 9, del D.L. n. 105/2019 (cfr. *infra*).

1.5.2 Il Decreto del presidente del Consiglio del Ministri 15 giugno 2021

La delega regolamentare contenuta nell'art. 1, comma 6, D.L. 21 n. 105/2019, con particolare riferimento alla lett. a) in materia di *individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica*, ha trovato ulteriore specificazione ad opera del D.P.C.M. 15 giugno 2021[33], che integra le disposizioni del regolamento adottato con il D.P.R. n. 54/2021.

In particolare, il D.P.C.M. 15 giugno 2021 individua le categorie in relazione alle quali i soggetti inclusi nel perimetro che intendano procedere[34] all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici delle pubbliche amministrazioni[35], effettuano la comunicazione al

[33] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 15 giugno 2021 *Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*.

[34] Anche per il tramite delle centrali di committenza alle quali sono tenuti a fare ricorso.

[35] A tal proposito si ricorda che l'art. 1, comma 1 lett. i), del D.P.R. 5 febbraio 2021, n. 54 definisce servizio informatico, un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di *cloud computing* di cui all'art. 3, comma 1, lettera aa), del decreto legislativo 18 maggio 2018, n. 65.

Centro di valutazione e certificazione nazionale CVCN o ai CV centri di valutazione del Ministero dell'interno e del Ministero della difesa.

L'art. 3 del D.P.C.M. chiarisce che le categorie sono individuate sulla base dei criteri tecnici di cui all'art. 13, comma 1, del D.P.R. n. 54/2021 (già esaminati nel par. 5.1.3). Inoltre, dette categorie sono contenute nell'elenco di cui all'allegato 1 dello stesso D.P.C.M. 15 giugno 2021.

ELENCO DELLE CATEGORIE (All. 1, al D.P.C.M. 15 giugno 2021)

Categoria	Bene, sistema, servizio
Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)	*Router* *Switch* *Repeater* Bilanciatori di carico *Traffic shaper* *Proxy* Ponte radio *Access Network* per reti Radiomobili 2G, 3G, 4G, 5G *Gateway Wifi* *Network Function* *Virtualization* (NFV): o *vSwitch* | o *vRouter* | o *Application Function* (5G)

	Optical transmission board *Multiservice Provisioning* *Platform* (MSPP) *Automotive ECU switch* (*Ethernet*, CAN, LIN) *IoT Edge Gateway*
Componenti *hardware* e *software* che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati	*Firewall* *Security Gateway* *Hardware Security Module* (HSM) *Intrusion Detection System* (IDS) *Intrusion Prevention System* (IPS) *Network Function* *Virtualization* (NFV) o *Authentication Server Function* (5G) o *Whitelisting* dei processi *Virtual Private Network* (VPN) *Trusted Platform Module*
Componenti *hardware* e *software* per acquisizione dati, monitoraggio supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali	Sistemi SCADA (*Supervisory Control And Data Acquisition*) *Manufacturing Execution Systems* (MES) *Software Defined Network* (SDN) Controller Sistemi *Artificial Intelligence* (AI) e *Machine Learning* (ML) per gestione reti/sistemi

	5G *Mobile Edge Computing* (MEC) NFV: o *Network Slice Selection Function* (5G) o *Application Function* (5G)| o *Policy Control Function* (5G) o *Unified Data Management* (5G) o *Session Management Function* (5G) *Management and Orchestration* (MANO) *IoT orchestrator*
Applicativi *software* per l'implementazione di meccanismi di sicurezza	Applicazioni informatiche per la sicurezza o *Public Key Infrastructure* (PKI) o *Single Sign-On* (SSO) o Controllo Accessi Moduli *software* che implementano *Web Service* mediante API, per protocolli di comunicazione

Il loro aggiornamento, ad opera di specifico decreto del Presidente del Consiglio dei ministri, avviene con cadenza almeno annuale, avuto riguardo all'innovazione tecnologica, nonché all'eventuale modifica dei criteri tecnici di cui all'art. 13, comma 1, del D.P.R. n. 54/2021.

1.6. I compiti del CVCN nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT

Il settimo comma dell'art. 1, D.L. n. 105/2019, precisa che 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, il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;

b) definisce le metodologie di verifica e di test e svolge le attività di verifica ed ispezione ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego. Ove necessario il CVCN detta anche prescrizioni di utilizzo al committente[36];

c) elabora e adotta, previo conforme avviso del *Tavolo interministeriale* 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.

1.7. Il regime sanzionatorio

L'art. 1, comma 9, del D.L. n. 105/2019 definisce il regime sanzionatorio per le ipotesi di inosservanza degli obblighi derivanti dall'appartenenza al perimetro di cybersicurezza nazionale. In particolare, la norma prevede che, salvo che il fatto costituisca reato:

[36] A tali fini il CVCN si avvale anche di laboratori che esso stesso ha provveduto ad accreditare secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri da adottarsi, su proposta del CIC, entro dieci mesi conversione in legge del D.L. n. 105/2019.

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

b) il mancato adempimento dell'obbligo di notifica degli incidenti, 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 volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

d) la mancata comunicazione di avvio delle procedure di affidamento 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, 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 da parte di fornitori di beni, sistemi e servizi destinati alle reti 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 è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

h) il mancato rispetto delle prescrizioni definite dal CVCN in materia di metodologie di verifica e di test è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in assenza della comunicazione o del superamento dei test, oltre alle sanzioni di cui ai punti d) ed e), comporta 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.

Il comma 11, dell'art. 1, D.L. n. 105/2019 prevede la reclusione da uno a tre anni per chiunque, allo scopo di ostacolare o condizionare l'espletamento delle attività ispettive e di vigilanza fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni di avvio delle procedure di affidamento, o per lo svolgimento delle attività ispettive e di vigilanza od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

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, per i fornitori di servizi fiduciari qualificati e per i gestori di posta elettronica certificata, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma. Ai fini dell'accertamento e dell'irrogazione di tali sanzioni trovano applicazione i principi generali in materia di sanzioni amministrative di cui al Capo I, Sezioni I e II, della L. 24 novembre 1981, n. 689.

Per i dipendenti dei soggetti pubblici inclusi nel perimetro di cybersicurezza nazionale, la violazione delle disposizioni di cui sin qui illustrate può costituire causa di *responsabilità disciplinare* e *amministrativo-contabile*.

La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni in materia di perimetro della sicurezza nazionale cibernetica può avvalersi dell'*Agenzia per l'Italia Digitale* (AgID) sulla base di apposite convenzioni.

Il comma 19-*bis*, dell'art. 1, D.L. n. 105/2019 attribuisce al Presidente del Consiglio dei ministri il coordinamento della coerente attuazione delle disposizioni in materia di perimetro di sicurezza nazionale cibernetica. In questa attività il presidente del Consiglio dei Ministri può avvalersi anche del *Dipartimento delle informazioni per la sicurezza*, che assicura gli opportuni raccordi con le autorità e i soggetti coinvolti.

1.8. Le Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica

Ai sensi dell'art. 5 del D.L. n. 105/2019, il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del *Comitato interministeriale per*

la sicurezza della Repubblica, *può comunque disporre*, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, *la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati*. Laddove in tali determinazioni sia recata deroga alle leggi vigenti, anche ai fini delle ulteriori necessarie misure correlate alla disattivazione o all'interruzione, le stesse determinazioni devono contenere l'indicazione delle principali norme a cui si intende derogare e tali deroghe devono essere specificamente motivate. Dette determinazioni non sono soggette) al controllo preventivo di legittimità di cui all'art. 3 della L. 14 gennaio 1994, n. 20, in materia di controllo della Corte dei conti.

Qualora il Presidente del Consiglio dei ministri eserciti poteri è tenuto ad informare, entro trenta giorni, il *Comitato parlamentare per la sicurezza della Repubblica* delle misure disposte.