

**SCHEMA DI DECRETO DEL PRESIDENTE DELLA REPUBBLICA 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.**

**IL PRESIDENTE DELLA REPUBBLICA**

Visto l'articolo 87, quinto comma, della Costituzione;

Visto l'articolo 17, comma 1, della legge 23 agosto 1988, n. 400;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e in particolare l'articolo 1, comma 6;

Visto l'articolo 29 del decreto legislativo 7 marzo 2005, n. 82;

Vista la legge 24 novembre 1981, n. 689;

Vista la legge 7 agosto 1990, n. 241;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del.....;

Udito il parere del Consiglio di Stato espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del .....

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del .....

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro dello sviluppo economico, di concerto con i Ministri dell'interno, della difesa, dell'economia e delle finanze e per l'innovazione tecnologica e la digitalizzazione;

**EMANA**

il seguente regolamento:

**Capo I**

**Disposizioni generali**

**ART. 1**

*(Definizioni)*

1. Ai fini del presente decreto si intende per:
  - a) decreto-legge: il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
  - b) perimetro: il perimetro di sicurezza nazionale cibernetica istituito ai sensi dell'articolo 1, comma 1, del decreto-legge;

- c) DPCM: il decreto del Presidente del Consiglio dei ministri che attua le disposizioni di cui all'articolo 1, comma 2, lettere a) e b), del decreto- legge;
- d) soggetti inclusi nel perimetro: i soggetti di cui all'articolo 1, comma 2, lettera a) del decreto- legge individuati sulla base dei criteri di cui all'articolo 4 del DPCM;
- e) compromissione: la perdita di sicurezza o di efficacia dello svolgimento di una funzione essenziale dello Stato o di un servizio essenziale, connessa al malfunzionamento, all'interruzione, anche parziali, ovvero all'utilizzo improprio di reti, sistemi informativi e servizi informatici;
- f) 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;
- g) analisi del rischio: un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale ai fini di cui all'articolo 1, comma 2, lettere a) e b), del decreto-legge, e conseguentemente di trattare tale rischio individuando e implementando idonee misure di sicurezza;
- h) rete, sistema informativo:
  - 1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera dd), del decreto legislativo 1° agosto 2003, n. 259;
  - 2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale;
  - 3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione, compresi i programmi di cui al numero 2);
- i) 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'articolo 3, comma 1, lettera aa), del decreto legislativo 18 maggio 2018, n. 65;
- l) categorie: tipologie di beni, sistemi o servizi ICT destinati ad essere impiegati sui beni ICT di cui all'elenco dell'articolo 7 del DPCM, individuate sulla base di criteri tecnici, la cui acquisizione è subordinata alla valutazione del CVCN;
- m) oggetto della fornitura: bene, sistema o servizio ICT, appartenente alle categorie, che il soggetto incluso nel perimetro intende acquisire;
- n) CVCN: il Centro di Valutazione e Certificazione nazionale, istituito presso il Ministero dello sviluppo economico, di cui all'articolo 1, comma 6, lettera a), del decreto-legge;
- o) CV: i centri di valutazione del Ministero dell'interno e del Ministero della difesa di cui all'articolo 1, comma 6, lettera a), del decreto-legge;
- p) LAP: laboratorio accreditato di prova, indipendente dai soggetti inclusi nel perimetro e dai fornitori, che ha ottenuto l'accreditamento dal CVCN ai sensi dell'articolo 1, comma 7 del decreto-legge;
- q) oggetto della valutazione: l'oggetto della fornitura sottoposto al procedimento di valutazione da parte del CVCN o dei CV;
- r) centrali di committenza: Consip S.p.A. e i soggetti aggregatori ai fini della realizzazione degli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208;
- s) fornitore: persona fisica o giuridica che fornisce l'oggetto della fornitura destinato alle reti, ai sistemi informativi e ai servizi informatici di cui all'articolo 1, comma 2, lett. b), del decreto- legge;

- t) evidenze: documenti, registrazioni, dati, constatazioni, dichiarazioni di fatti, reportistica, attività, procedure, o altre informazioni utili ad attestare l'adempimento degli obblighi previsti dal decreto-legge;
- u) verifica: attività di analisi e controllo documentale delle evidenze al fine di accertare l'adempimento degli obblighi previsti dal decreto-legge;
- v) ispezione: 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 decreto-legge;
- z) autorità competenti: le autorità che, ai sensi dell'articolo 1, comma 6, lettera c), del decreto-legge, dispongono ed effettuano verifiche e ispezioni;
- aa) personale incaricato: il personale incaricato dalle Autorità competenti dello svolgimento delle verifiche e delle ispezioni.

## ART. 2

*(Ambito di applicazione)*

1. Il presente decreto, in attuazione dell'articolo 1, comma 6, lettere a), b) e c), del decreto-legge, definisce:
  - a) le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del CVCN e dei CV, ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri di cui alla lettera b) del presente articolo, fatti salvi i casi di deroga di cui all'articolo 1, comma 6, lettera a), del decreto-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, ad eccezione di quelle riguardanti 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 ai sensi dell'articolo 1, comma 6, lettera c), del decreto-legge.

## CAPO II

### **Procedura di valutazione del CVCN e dei CV**

## ART. 3

*(Comunicazione di affidamento)*

1. I soggetti inclusi nel perimetro, prima dell'avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione di contratti relativi alla fornitura di beni, sistemi e di servizi ICT di cui all'articolo 1, comma 6, lettera a), del decreto-legge, anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza, ne danno comunicazione al CVCN o al CV.

2. La comunicazione è trasmessa in via telematica al CVCN o al CV per le valutazioni di rispettiva competenza del CVCN o dei CV. I dati contenuti nelle comunicazioni sono raccolti in archivi informatici istituiti presso le Amministrazioni nelle quali operano il CVCN e i CV.
3. La comunicazione di cui al comma 1, oltre ai dati identificativi del soggetto incluso nel perimetro, contiene i seguenti elementi:
  - a) la descrizione generale dell'oggetto di fornitura;
  - b) l'impiego, ovvero destinazione d'uso dell'oggetto di fornitura nell'ambito dei beni ICT di cui all'articolo 7 del DPCM;
  - c) la categoria di appartenenza dell'oggetto di fornitura;
  - d) le informazioni e i servizi che l'oggetto di fornitura deve trattare e le relative modalità di gestione;
  - e) le informazioni relative all'eventuale acquisizione mediante gli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208.
4. In aggiunta agli elementi di cui al comma 3, la comunicazione include il documento di analisi del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. 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 di fornitura, espressi in termini di capacità di proteggere la disponibilità, l'integrità e la riservatezza delle informazioni e i servizi di cui al comma 3, lettera d).
5. Con successivo atto del CVCN, da adottarsi entro 60 giorni dalla data di entrata in vigore del presente decreto, sono definite le metodologie per la predisposizione del documento di analisi del rischio e per l'individuazione dei livelli di severità dei test di cui all'articolo 5, comma 2.
6. Ai fini del comma 5, il CVCN, sulla base di standard tecnici di riferimento, tiene conto dell'impatto di violazioni intenzionali o accidentali sui requisiti di sicurezza, di cui alla lettera b) del comma 4, che determinano eventi di indisponibilità, malfunzionamento e compromissione della funzione essenziale o del servizio essenziale.

#### ART. 4

##### *(Procedimento di verifica e valutazione)*

1. Il CVCN o i CV avviano il procedimento di verifica e valutazione dell'analisi documentale contenuta nella comunicazione di cui all'articolo 3.
2. Il procedimento si articola in:
  - a) verifiche preliminari, imposizione di condizioni e di test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, di cui all'articolo 5;
  - b) fase di preparazione all'esecuzione dei test, di cui all'articolo 6;
  - c) esecuzione dei test di hardware e di software e definizione di eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro, di cui agli articoli 7 e 8.

3. Le attività di cui alla lettera a) del comma 2 sono svolte entro il termine di quarantacinque giorni dalla comunicazione di cui all'articolo 3, prorogabile una sola volta di quindici giorni nei casi di particolare complessità, laddove l'oggetto di valutazione:
  - a) è costituito da beni, sistemi e servizi ICT integrati tra di loro;
  - b) è 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.
4. Le attività di cui alla lettera c) del comma 2 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 secondo le condizioni individuate ai sensi dell'articolo 5, commi 5 e 6.
5. Decorsi i termini di cui al comma 3 senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento. Decorsi i termini di cui al comma 4, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire l'esecuzione del contratto.
6. Ai fini dello svolgimento delle attività di cui al comma 2, lettera c), il CVCN può avvalersi di LAP e si coordina, ove previsto, con i centri di valutazione del Ministero dell'Interno e del Ministero della Difesa, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge.
7. Il CVCN condivide con i CV e i LAP le metodologie per l'effettuazione dei test ai sensi del decreto del Presidente del Consiglio dei ministri adottato in attuazione dell'articolo 1, comma 7, lettera b), del decreto-legge. Il CVCN, i CV e i LAP assicurano, anche con strumenti adeguati, la riservatezza di tali metodologie.
8. 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'articolo 1, comma 1, del decreto-legge.

## ART.5

### *(Verifiche preliminari, individuazione di condizioni e test)*

1. A seguito della comunicazione di cui all'articolo 3, il CVCN o i CV effettuano verifiche preliminari ed eventualmente comunicano 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. 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 ai sensi dell'articolo 6, comma 1, lettera b), della legge 7 agosto 1990, n. 241.
2. Nell'individuazione dei test da eseguire, il CVCN e i CV tengono conto dell'analisi del rischio di cui all'articolo 3 e dei livelli di severità determinati sulla base della metodologia di cui al comma 5 del medesimo articolo 3.
3. 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.
4. Con atto del CVCN, da adottarsi entro 60 giorni dalla data di entrata in vigore del presente decreto, sono definiti i test corrispondenti ai livelli di severità derivanti dall'analisi del rischio di cui all'articolo 3.
5. 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 di cui all'articolo 3, comma 4, lettera b);
  - 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 di test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.
6. Il CVCN e i CV comunicano 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.
  7. Le centrali di committenza, ai fini della realizzazione degli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, tengono conto delle previsioni di cui all'articolo 1, comma 6, del decreto-legge, e di cui al presente decreto, con riferimento alle acquisizioni di beni, sistemi e servizi ICT inclusi nelle categorie di cui all'articolo 1, lettera l), e di cui al capo III del presente decreto. Al fine dell'effettuazione di tali acquisizioni mediante i detti strumenti, i soggetti pubblici inclusi nel perimetro specificano, secondo quanto previsto nella relativa documentazione di gara e tenendo conto delle caratteristiche della specifica acquisizione, gli elementi relativi a condizioni e a test di cui al comma 6. Gli aggiudicatari assicurano il rispetto di dette previsioni.
  8. 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.
  9. 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.

## ART. 6

### *(Preparazione all'esecuzione dei test)*

1. A seguito della comunicazione di cui al comma 9 dell'articolo 5, il CVCN e i CV verificano, 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 sono in corso valutazioni, secondo le modalità dell'articolo 7. Nel caso in cui:
  - a) l'oggetto è stato sottoposto a precedenti valutazioni o è in corso di valutazione, sono effettuate le verifiche di cui al comma 2, finalizzate a evitare la duplicazione di test eventualmente già eseguiti;
  - b) l'oggetto non è stato sottoposto a precedenti valutazioni e non è in corso di valutazione, si procede come descritto al comma 3.

2. Nei casi di cui al comma 1, lettera a), ferme restando le condizioni di cui all'articolo 5, 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 di cui all'articolo 5, comma 6, lettera a), sia i test di intrusione di cui all'articolo 5, comma 6, lettera b);
  - 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.
3. Nei casi di cui al comma 1, lettera a), diversi dal comma 2, ferme restando le condizioni di cui all'articolo 5, 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.
4. Nei casi di cui al comma 1, lettera b), e di cui al comma 3:
  - 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 di cui all'articolo 5 e definiscono la sede in cui svolgere tali attività.
5. Nei casi di cui al comma 2, il CVCN o i CV, ferma restando la possibilità di prevedere le prescrizioni di utilizzo di cui all'articolo 8, comunicano al soggetto incluso nel perimetro, e per conoscenza al fornitore, la conclusione del procedimento.

## ART.7

### *(Esecuzione dei test)*

1. Concluse le attività preliminari di cui all'articolo 6, il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel perimetro e al fornitore. I test si concludono entro i termini individuati dall'articolo 4, comma 4.
2. Con la comunicazione di cui al comma 1 il CVCN o i CV specificano le modalità di collaborazione dei fornitori durante l'esecuzione delle prove.
3. I test sono eseguiti presso i laboratori del CVCN, dei CV e dei LAP. Se necessario, possono essere eseguiti da personale del CVCN, dei CV e dei LAP presso il fornitore o il soggetto incluso nel perimetro.
4. I test sono effettuati secondo le metodologie predisposte dal CVCN di cui dall'articolo 4, comma 7, assicurando il rispetto di quanto previsto all'articolo 4, comma 8. I CV e i LAP sono tenuti a non divulgare tali metodologie.
5. Ai sensi dell'articolo 10 bis della legge 7 agosto 1990, n. 241, 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. Entro il termine di dieci giorni dalla ricezione della comunicazione, il fornitore può provvedere a risolvere il malfunzionamento. La predetta comunicazione interrompe i termini di cui all'articolo 4, comma 4, 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.

6. 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.
7. I LAP, eventualmente incaricati per l'esecuzione dei test, trasmettono il rapporto di prova al CVCN entro 7 giorni lavorativi dalla scadenza dei termini per l'esecuzione dei test.
8. 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.

## ART. 8

### *(Esito della valutazione e prescrizioni di utilizzo)*

1. Sulla base del rapporto di prova di cui all'articolo 7, commi 7 e 8, il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test. Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro i termini di cui all'articolo 4, comma 4.
2. In caso di esito negativo del rapporto di valutazione, il CVCN e i CV provvedono ai sensi dell'articolo 10-bis della legge 7 agosto 1990, n. 241.
3. Nel caso in cui l'esito di cui al comma 1 sia positivo, il CVCN può imporre al soggetto incluso nel perimetro prescrizioni per l'utilizzo dell'oggetto dell'affidamento ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge.
4. Le prescrizioni di cui al comma 3 possono riguardare ~~tra l'altro~~ anche il mantenimento nel tempo del livello di sicurezza nell'ambiente di esercizio.

## ART. 9

### *(Oneri economici a carico del fornitore)*

1. Le spese a carico del fornitore per le attività di valutazione svolte dal CVCN e dai CV sono calcolate sulla base delle disposizioni contenute nel decreto del Ministro delle comunicazioni 15 febbraio 2006, pubblicato nella Gazzetta Ufficiale n. 82 del 7 aprile 2006.
2. I LAP fanno riferimento al decreto di cui al comma 1 ai fini della determinazione dei costi relativi all'esecuzione dei test

## ART. 10

### *(Casi di deroga)*

1. Nel rispetto dell'articolo 1, comma 6, lettera a), ultimo periodo, del decreto-legge, non sono tenute agli obblighi di comunicazione previsti dal presente decreto le Autorità di pubblica sicurezza e le forze di polizia di cui agli articoli 1, 13, 14, 15 e 16, della legge 1° aprile 1981, n. 121.
2. Ai sensi dell'articolo 1, comma 6, lettera a), del decreto-legge, ai fini della deroga alla comunicazione di cui all'articolo 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) apparati e sistemi informatici;
- c) apparati e sistemi di rete e telecomunicazioni;
- d) servizi di connettività;
- e) servizi di gestione, assistenza e manutenzione degli apparati, dei sistemi e delle reti di cui alle lettere a), b), c) e d).

3. L'elenco e la documentazione relativa agli affidamenti effettuati ai sensi del comma 2 sono resi disponibili per le verifiche e le ispezioni di cui al capo IV del presente decreto.

4. Nei casi di cui al presente articolo è comunque garantito l'utilizzo di beni, sistemi e servizi ICT conformi alle misure di sicurezza di cui all'articolo 1, comma 3, lettera b), del decreto-legge.

#### ART. 11

*(Periodo transitorio)*

1. Il CVCN e i CV individuano i test da eseguire secondo un approccio gradualmente crescente nelle verifiche di sicurezza ai sensi dell'articolo 1, comma 6, del decreto-legge. Nei primi 18 mesi dalla data di entrata in vigore del presente decreto, ferma restando la possibilità di imporre le condizioni di cui all'articolo 5 e le prescrizioni di utilizzo di cui all'articolo 8, nonché di effettuare l'analisi documentale di cui all'articolo 4, il CVCN e i CV possono effettuare test con livello di complessità crescente nel tempo, secondo un programma contenuto nell'atto di cui all'articolo 5, comma 4.

#### ART. 12

*(Casi particolari)*

1. Ai sensi dell'articolo 3, comma 2, del decreto-legge, la valutazione preventiva per l'esercizio dei poteri speciali di cui all'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni dalla legge 11 maggio 2012, n. 56, è effettuata secondo le procedure, le modalità e i termini di cui all'articolo 1, comma 6, del decreto-legge, ed al presente decreto.

### **CAPO III**

#### **Categorie di tipologie di beni, sistemi e servizi ICT**

#### ART. 13

*(Criteri tecnici per l'individuazione delle categorie)*

1. Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN 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.
2. Le categorie, sulla base dei criteri di cui al comma 1, sono individuate con decreto del Presidente del Consiglio dei ministri, ai sensi dell' articolo 1, comma 6, lettera a), del decreto-legge.

## **CAPO IV**

### **Ispezioni e verifiche**

#### ART. 14

*(Oggetto delle verifiche e delle ispezioni)*

1. Le verifiche e le ispezioni hanno lo scopo di accertare, nell'ambito di quanto previsto dal presente decreto, 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 ai sensi dell'articolo 1, comma 2, lettera b) , del decreto-legge;
  - 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 dal relativo decreto attuativo;
  - c) adozione delle misure di sicurezza di cui all'articolo 1, comma 3, lettera b) , del decreto-legge, nei termini e con le modalità previste dal relativo decreto attuativo;
  - d) comunicazione al CVCN di cui all'articolo 1, comma 6, lettera a) , del decreto-legge, nei termini e con le modalità previste dal presente decreto;
  - 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 ai sensi dell'articolo 1, comma 6, lettera a) , del decreto-legge;
  - f) collaborazione per l'effettuazione delle attività di test da parte dei soggetti ai sensi dell'articolo 1, comma 6, lettera b) , del decreto-legge;
  - g) osservanza delle prescrizioni formulate dalle Autorità competenti ai sensi dell'articolo 1, comma 6, lettera c) , del decreto-legge , all'esito delle attività di ispezione e verifica;

- h) osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto ai sensi dell'articolo 1, comma 7, lettera b) , del decreto-legge.

## ART. 15

### *(Autorità competenti)*

1. Ai sensi dell'articolo 1, comma 6, lettera c), del decreto-legge, le verifiche e le ispezioni sono disposte ed effettuate:
  - a) dalla Presidenza del Consiglio dei Ministri, per i profili di pertinenza dei soggetti inclusi nel perimetro pubblici e di quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, rientranti tra i soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge, ed in particolare dalla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione;
  - b) dal Ministero dello Sviluppo Economico per i soggetti privati inclusi nel perimetro e di cui al medesimo articolo 1, comma 2-bis, del decreto-legge, ed in particolare dalla struttura competente in materia di tecnologie delle comunicazioni e di sicurezza informatica.
2. Le Autorità competenti istituiscono e aggiornano un elenco del personale da incaricare per lo svolgimento delle attività di ispezione e verifica che, ove necessario, deve essere in possesso della abilitazione di sicurezza di cui al decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5.
3. Ai fini dello svolgimento delle verifiche e delle ispezioni, le Autorità competenti nominano il personale incaricato, nonché un responsabile del procedimento competente per lo svolgimento dell'istruttoria, ai sensi dell'articolo 6 della legge 7 agosto 1990, n. 241.
4. Nell'attribuzione degli incarichi le Autorità competenti per l'accertamento si attengono a criteri di professionalità e di rotazione.
5. Ai sensi dell'articolo 6 bis della legge 7 agosto 1990, n. 241, 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.
6. Ai sensi dell'articolo 1, comma 8, lettera a), del decreto-legge, le Autorità competenti si raccordano, ove necessario per lo svolgimento delle verifiche e delle ispezioni, con le autorità di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65, anche al fine di avvalersi di personale dipendente esperto nei settori di cui al medesimo decreto legislativo.

## ART. 16

### *(Attività di verifica e ispezione)*

1. Le Autorità competenti dispongono verifiche e ispezioni sulla base degli atti di programmazione dalle medesime adottati, nonché in caso di ulteriori esigenze derivanti da:

- a) notifiche di incidenti ai sensi dell'articolo 1, comma 3, lettera a), del decreto-legge;
  - b) rilevate difformità rispetto agli obblighi imposti dal decreto-legge e dai relativi decreti attuativi;
  - c) segnalazioni provenienti da altre Autorità Pubbliche.
2. Le ispezioni possono essere svolte successivamente alle verifiche qualora si ritenga necessario riscontrare le evidenze analizzate, ovvero qualora le stesse presentino elementi tali da richiederne un approfondimento.
  3. Il responsabile del procedimento di cui all'articolo 15, comma 3, comunica ai soggetti inclusi nel perimetro l'avvio del procedimento di verifica o di ispezione con le modalità di cui all'articolo 8 della legge 7 agosto 1990, n. 241.
  4. I soggetti inclusi nel perimetro nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per lo svolgimento delle attività di cui al comma 1, comunicandone il nominativo al responsabile del procedimento.
  5. Il procedimento di verifica si conclude entro il termine di 90 giorni dal ricevimento delle evidenze richieste ai soggetti inclusi nel perimetro.
  6. Il procedimento di ispezione si conclude entro il termine di 60 giorni dalla data di avvio delle attività ispettive presso le sedi utilizzate dai soggetti inclusi nel perimetro.
  7. All'esito dell'attività di cui al comma 1, le Autorità competenti possono formulare specifiche prescrizioni a cui i soggetti inclusi nel perimetro devono attenersi. Il rispetto delle prescrizioni può essere oggetto di successiva attività di verifica e ispezione.

## ART. 17

### *(Attività di verifica)*

1. 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.
2. Il responsabile del procedimento formula le richieste di informazioni e di produzione delle evidenze all'incaricato di cui all'articolo 16, comma 4, che, entro 30 giorni dalla ricezione della richiesta, deve rendere disponibile quanto richiesto, secondo le modalità indicate.
3. Fatti salvi i casi di inadempimento degli obblighi di cui all'articolo 19, comma 2, durante l'esecuzione delle attività di cui al comma 1, il responsabile del procedimento può richiedere chiarimenti e integrazioni qualora le evidenze risultino incomplete o incongruenti. Entro 15 giorni dalla ricezione della richiesta, il soggetto deve fornire quanto richiesto, secondo le modalità indicate. La richiesta di chiarimenti o integrazioni sospende il termine di conclusione del procedimento.
4. Dell'attività svolta nel corso delle verifiche è redatto apposito verbale che il personale incaricato trasmette al responsabile del procedimento.

5. Qualora nel corso della verifica vengano in rilievo evidenze 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 documentazione ispettiva concernente fatti che possono integrare violazioni di disposizioni normative.

## ART.18

### *(Attività di ispezione)*

1. Le ispezioni si articolano nelle seguenti attività:
  - a) riscontro delle evidenze acquisite ove le stesse presentino elementi meritevoli di approfondimento;
  - b) analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari;
  - c) esame dei chiarimenti richiesti ai sensi dell'articolo 17, comma 3.
2. Per lo svolgimento delle attività di cui al comma 1, il personale incaricato può richiedere o eventualmente acquisire tutte le evidenze ritenute utili ai fini dell'accertamento.
3. Le ispezioni possono essere effettuate presso le sedi utilizzate dai soggetti inclusi nel perimetro nei casi di cui all'articolo 16, comma 1. L'intenzione di effettuare un'ispezione è comunicata dal responsabile del procedimento ai soggetti inclusi nel perimetro con un preavviso non inferiore a 15 giorni. La comunicazione 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.
4. Entro 7 giorni dalla ricezione della comunicazione di cui al comma 3, il soggetto può proporre date alternative a quelle previste per l'ispezione, individuando un termine non superiore a 15 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 7 giorni prima della prima data prevista per l'ispezione.
  - b) proporre un ulteriore piano e notificarlo nuovamente al soggetto con le stesse modalità del precedente; tale nuova pianificazione non può essere soggetta a richiesta di pianificazione alternativa da parte del soggetto e si intende confermata.
5. In mancanza della proposta di cui alla lettera a) del comma 4, le date delle ispezioni si intendono confermate.
6. Almeno 7 giorni prima dell'ispezione prevista, il soggetto comunica il nominativo dell'incaricato di cui all'articolo 16, comma 4.
7. Durante il corso dell'ispezione, i soggetti inclusi nel perimetro mettono a disposizione tutte le risorse richieste e 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 cui al comma 3.

8. Qualora durante il corso dell'ispezione emergano evidenze meritevoli di approfondimento, le stesse possono essere esaminate in una fase successiva.
9. Dell'attività svolta nel corso dell'ispezione è redatto apposito processo verbale da parte del personale incaricato che lo sottoscrive unitamente all'incaricato di cui all'articolo 16, comma 4. Qualora quest'ultimo si rifiuti di sottoscrivere il verbale, il personale incaricato ne dà evidenza nel verbale. Una copia del verbale è rilasciata al predetto soggetto che ha rifiutato la sottoscrizione e una copia è trasmessa al responsabile del procedimento.
10. Qualora nel corso dell'ispezione vengano in rilievo evidenze 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 documentazione ispettiva concernente fatti che possano integrare violazioni di disposizioni normative.

#### ART. 19

*(Esiti delle attività di verifica e di ispezione)*

1. L'Autorità competente, raccolti gli esiti delle attività di cui all'articolo 16, adotta il provvedimento di conclusione del procedimento, dandone comunicazione all'interessato, e, nei casi previsti, procede all'applicazione delle sanzioni di cui all'articolo 1, comma 9, del decreto-legge.

#### ART. 20

*(Invarianza finanziaria)*

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri per la finanza pubblica e le amministrazioni pubbliche interessate vi provvedono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

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.