**Relazione illustrativa**

Il decreto-legge 21 settembre 2019, n. 105, convertito nella legge n. 133/2019, di seguito indicato come decreto-legge, ha introdotto misure urgenti in materia di perimetro di sicurezza nazionale cibernetica e disposizioni riguardanti la disciplina dei poteri speciali nei settori di rilevanza strategica.

In particolare, il comma 6 dell’articolo 1, lettere a), b) e c) del decreto-legge demanda a un regolamento – da emanare ai sensi dell’articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge – la definizione di procedure, modalità e termini:

1. ai quali devono attenersi i pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che intendano procedere 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 individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico. Si tratta, in particolare, dei beni appartenenti a categorie individuate da un decreto del Presidente del Consiglio dei ministri sulla base di criteri tecnici che dovrà essere emanato entro 10 mesi dall'entrata in vigore della norma di conversione del decreto. Il processo di verifica è effettuato dal Centro di valutazione e certificazione nazionale (CVCN) - istituito presso il Ministero dello sviluppo economico - con riferimento ai soggetti pubblici e privati o dai Centri di valutazione del Ministero della difesa e del Ministero dell’interno per le acquisizioni rispettivamente destinate alle proprie reti, sistemi informativi e servizi informatici. Sono definiti i termini per le fasi di individuazione di test e condizioni per la valutazione dell’oggetto di fornitura e per l’esecuzione dei test, decorsi i quali i soggetti inclusi nel perimetro possono proseguire nella procedura di accertamento Sono stati esclusi gli approvvigionamenti necessari per le attività di prevenzione accertamento e repressione dei reati ed è stato previsto di demandare al decreto attuativo la disciplina dei casi di deroga per le forniture in sede estera.
2. con cui i fornitori dei suddetti beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti assicurano al CVCN e ai Centri di valutazione del Ministero della difesa e del Ministero dell’interno, per quanto di rispettiva competenza, la propria collaborazione per l’effettuazione delle attività di test, sostenendone gli oneri.
3. con cui il Ministero dello sviluppo economico e alla Presidenza del Consiglio dei Ministri, negli ambiti rispettivamente assegnati loro nel perimetro, svolgono le attività di ispezione e verifica in relazione a quanto previsto dal decreto-legge. In tale contesto, in considerazione delle specificità, le attività di verifica e ispezione riguardanti le reti, sistemi e servizi connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell’ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, sono svolte, senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché in tema di prevenzione e 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.

La proposta di decreto allegata si propone pertanto di dare attuazione alle disposizioni di cui all’articolo 1, comma 6, lettere a), b), e c) sopra indicate.

La proposta si compone di 4 Capi:

* **CAPO I: Disposizioni generali**
* **CAPO II:** **Procedura di valutazione del CVCN e dei CV**
* **CAPO III:** **Categorie di tipologie di beni, sistemi e servizi ICT**
* **CAPO IV: Ispezioni e verifiche**

Il Capo I “Disposizioni generali” si compone di due articoli.

**L’articolo 1 ”Definizioni”** comprende alcune definizioni riguardanti l’ambito del decreto-legge e indicate nello schema di decreto di attuazione dell’articolo 1, comma 2 del medesimo decreto-legge e ne introduce ulteriori utili a dare una migliore comprensione del testo del decreto. In particolare, sono definiti i soggetti individuati per le attività di valutazione e di test: il CVCN, i Centri di valutazione ed i Laboratori accreditati di prova (LAP). Inoltre, viene definita la Centrale di committenza per il cui tramite un soggetto pubblico incluso nel perimetro può effettuare acquisizioni di beni, sistemi e servizi ICT. Si evidenzia la definizione relativa alle categorie che vanno a specificare le tipologie di beni, sistemi e servizi. Sono altresì fornite le definizioni connesse alle attività di ispezione e verifica condotte dal Ministero dello sviluppo economico e dalla Presidenza del Consiglio dei Ministri, indicate come Autorità competenti.

**L’articolo 2 “Ambito di applicazione”**  precisa che scopo del decreto è dare attuazione all’articolo 1, comma 6, lettere a), b) e c) del decreto-legge, attraverso la definizione delle procedure, modalità e termini con cui il CVCN ed i CV valutano i beni, sistemi e servizi ICT che i soggetti inclusi nel perimetro che intendono acquisire nel caso in cui essi siano destinati ad di rilevanza strategica per la fornitura di servizi essenziali e per assicurare le funzioni essenziali dello Stato. Con l’obiettivo di precisare i beni, sistemi e servizi ICT da sottoporre alla valutazione del CVCN, il decreto ha lo scopo di stabilire criteri di natura tecnica per l’individuazione delle categorie, ovvero all’elenco di beni, sistemi e servizi ICT a cui si applica la procedura di valutazione. Inoltre, il decreto definisce 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.

Il CAPO II “Procedura di valutazione del CVCN e dei CV” si compone di nove articoli, dall’articolo 3 all’articolo 12.

**L’articolo 3 “Comunicazione di affidamento”** precisa i contenuti della comunicazione e le relative modalità di trasmissione al CVCN o ai CV, con la quale i soggetti inclusi nel perimetro manifestano l’intenzione di acquisire beni, sistemi e servizi ICT ai sensi dell’articolo 1, comma 6, lettera a) del decreto-legge.

La comunicazione contiene informazioni utili a comprendere, tra l’altro, le informazioni e i servizi che l’oggetto di fornitura deve trattare e le relative modalità di gestione e la sua destinazione d’uso. Nel caso in cui il soggetto incluso nel perimetro sia una PA la comunicazione fornisce indicazioni sul ricorso agli strumenti di acquisto e di negoziazione centralizzati utilizzati di cui all’articolo 1, comma 512, della legge 28 dicembre 2015, n. 208.

La comunicazione include altresì il documento di analisi del rischio associato all’oggetto della fornitura, che specifica l’ambiente operativo dell’ambito di impiego e i requisiti di sicurezza che caratterizzano il medesimo impiego.

Le metodologie per la predisposizione del documento di analisi del rischio sono definite, sulla base di standard tecnici di riferimento, con successivo atto del CVCN, da emanarsi entro 60 giorni dall’entrata in vigore del presente decreto. Con il medesimo atto è definita la corrispondenza tra l’analisi del rischio ed i livelli di severità dei test che sono eseguiti dal CVCN o dai CV.

**L’art. 4 “Procedimento di verifica e valutazione”** sintetizza le tre fasi di verifica condotte dal CVCN e dai CV, dettagliate nei successivi articoli. La prima fase si avvia con l’analisi della comunicazione trasmessa dal soggetto incluso nel perimetro e si conclude con l’individuazione di test e condizioni da includere nei bandi di gara o nei contratti. Una volta noto il fornitore e l’oggetto in modo univoco, la seconda fase prevede l’attività di preparazione all’esecuzione dei test per la quale non sono previsti termini, riguardando un’attività che il fornitore deve porre in essere per rendere possibile l’esecuzione dei test e pertanto indipendente dal CVCN e dai CV. Infine, la terza fase comprende l’esecuzione dei test e decorre dalla data in cui siano terminate le attività propedeutiche all’esecuzione dei test. I termini per la prima e la terza fase confermano quelli stabiliti dal decreto-legge, pari rispettivamente a 45 giorni (prorogabili una sola volta di quindici giorni in casi di particolare complessità) e 60 giorni. Il comma 3 individua i casi di particolare complessità e il comma 5 ribadisce, ai sensi del decreto-legge, che decorsi i termini del presente articolo senza una pronuncia del CVCN o dei CV, i soggetti inclusi nel perimetro possono proseguire l’esecuzione del contratto. L’articolo conferma la possibilità per il CVCN di avvalersi di Laboratori accreditati per l’esecuzione dei test e la realizzazione di un raccordo tra CVCN e CV per evitare duplicazioni di test. I Laboratori accreditati e i CV utilizzano le metodologie per l’effettuazione dei test predisposte dal CVCN e ne assicurano la riservatezza.

**L’art.5 “Verifiche preliminari, individuazione di condizioni e test”** definisce le disposizioni relative alla prima fase di verifica e valutazione, che prevede inizialmente l’analisi della documentazione fornita con la comunicazione. 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. Conclusa l’analisi della documentazione, il CVCN e i CV possono individuare test da eseguire che rientrano in due tipologie definite al comma 3. Il dettaglio dei test corrispondenti ai tre livelli di severità derivanti dall’analisi del rischio sono, invece, definiti con atto del CVCN da adottarsi entro 60 giorni dall’entrata in vigore del decreto. Nel caso in cui sia prevista l’esecuzione dei test, il fornitore deve assicurare il rispetto delle condizioni di cui al comma 5 ed eventuali ulteriori condizioni indispensabili per l’esecuzione dei test. 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.

In particolare, al comma 7 al fine di garantire il raccordo fra la disposizione che pone l’obbligo di ricorso per le pubbliche amministrazioni agli strumenti centralizzati di Consip e dei soggetti aggregatori e il rispetto della normativa in tema di sicurezza cibernetica, si dispone che le centrali di committenza inseriscano previsioni e misure volte a disciplinare lo svolgimento di tutte le attività necessarie, anche a carico del fornitore, per le verifiche da parte del CVCN, prevedendo anche le specificazioni che dovranno essere inserite dai soggetti pubblici inclusi nel perimetro che ricorrono agli strumenti medesimi. Ciò in quanto le attività di valutazione del rischio e le previsioni di condizioni e test presuppongono necessariamente una valutazione concreta dell’acquisizione in relazione al contesto in cui questa andrà ad operare. Successivamente all’aggiudicazione della gara o della stipula del contratto, il soggetto incluso nel perimetro 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.

**L’ art. 6 “Preparazione all’esecuzione dei test”** definisce le modalità di interazione tra CVCN e CV prima della definizione puntuale dei test da eseguire. Tale raccordo, attraverso una piattaforma informatica da realizzare presso il Ministero dello sviluppo economico, consente di evitare la duplicazione delle attività di test. A seguito dell’interazione, qualora uno dei Centri di valutazione abbia già effettuato o stia effettuando test con livello di severità uguale o maggiore rispetto a quello richiesto, non saranno richiesti ulteriori test. In questo caso, ferma restando la possibilità di prevedere specifiche condizioni per il fornitore e prescrizioni per il soggetto incluso nel perimetro, la procedura si chiude con la comunicazione al soggetto incluso nel perimetro e al fornitore. Se invece i test ad un livello di severità inferiore sono stati eseguiti dal CVCN o da CV o sono in corso test di livello di severità inferiore, sono individuati gli ulteriori test da effettuare. Infine, se nessun test è stato eseguito o non sono in corso di esecuzione test, sono individuati i test da eseguire. In tali ultimi due casi 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. Il CVCN può affidare l’esecuzione dei test ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore.

**L’art.7 “Esecuzione dei test”** prevede che a conclusione delle attività preliminari il CVCN o i CV comunichino l’avvio dei test al soggetto incluso nel perimetro e al fornitore, specificando le modalità di collaborazione dei fornitori durante l’esecuzione delle prove. I test sono eseguiti secondo le metodologie predisposte dal CVCN presso i laboratori del CVCN, dei CV o dei Laboratori accreditati di prova. Se necessario, possono essere eseguiti da personale del CVCN, dei CV e dei LAP presso il fornitore o il soggetto incluso nel perimetro. Si ricorre all’articolo 10 bis della legge n. 241 del 1990, 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, 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 7 giorni lavorativi dalla scadenza dei termini per l’esecuzione dei test.

**L’art. 8 “Esito della valutazione e prescrizioni di utilizzo” stabilisce che sulla** base del rapporto di prova 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 previsti. 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. **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. Tali prescrizioni di cui al comma 3 possono riguardare tra l’altro il mantenimento nel tempo del livello di sicurezza nell’ambiente di esercizio.

**L’art. 9 “Oneri economici a carico del fornitore”** prevede che 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 15 febbraio 2006 del Ministro delle comunicazioni di concerto con il Ministro dell’economia e delle finanze, pubblicato in Gazzetta Ufficiale n. 82 del 7 aprile 2006. Anche i LAP fanno riferimento al decreto di cui al comma 1 ai fini della determinazione dei costi dell’esecuzione dei test. Tali disposizioni sono finalizzate ad assicurare una modalità uniforme per il calcolo degli oneri posti a carico dei fornitori evitando che i fornitori debbano sostenere oneri diversi a fronte dell’esecuzione dei medesimi test.

**L’art. 10 “Casi di deroga”** nel rispetto dell’art. 1, comma 6, lett a), ultimo periodo del decreto legge,conferma l’esclusione dal campo di applicazione del decreto degli 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 di competenza delle Autorità di pubblica sicurezza e delle forze di polizia, precisando la normativa di riferimento che consente di individuare l’ambito dell’esenzione. L’articolo individua inoltre i casi in cui è considerato indispensabile procedere in sede estera, all’acquisizione di forniture di 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.

In ogni caso è garantito l’utilizzo di beni, sistemi e servizi ICT conformi alle misure di sicurezza di cui al comma 3, lettera b), del decreto-legge ed è assicurata la disponibilità dell'elenco e della documentazione relativa agli affidamenti effettuati all’estero per le verifiche e le ispezioni per l’accertamento del rispetto degli obblighi previsti dal decreto-legge.

**L’art. 11 “Periodo transitorio”** prevede cheIl CVCN e i CV individuino 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 dall’entrata in vigore del presente decreto, il CVCN e i CV possono effettuare test con livello di complessità crescente nel tempo, secondo un programma contenuto nell’atto di cui all’art. 5, comma 4 che definisce i test corrispondenti ai livelli di severità derivanti dall’analisi del rischio di cui all’articolo 3.

**L’art. 12 “Casi particolari”** precisa che 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 dal CVCN secondo le procedure, le modalità e i termini di cui all’art.1, comma 6 del decreto legge nonché al presente decreto, ai sensi dell’articolo 3, comma 2, del decreto-legge. Il presente articolo attua quindi la prescrizione dell’art. 3, comma 2, del decreto legge in combinato disposto con l’art. 1,comma 6 del decreto legge stesso e dell’art. 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni dalla legge 11 maggio 2012, n. 56, consentendo , pertanto, di effettuare i test tecnici per la valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l’integrità e la sicurezza delle reti e dei dati che vi transitano, in modo omogeneo ed armonizzato con le procedure, modalità e termini stabiliti dall’art. 1, comma 6 come attuati dal presente decreto.

Il Capo III “Categorie di tipologie di beni, sistemi e servizi” ICT contiene l’articolo 13.

**L’art. 13 “Criteri tecnici per l’individuazione delle categorie”** definisce i criteri tecnici per l’individuazione delle categorie di beni, sistemi e servizi ICT che sottostanno alla valutazione del CVCN e dei CV. Tali criteri si basano sull’esecuzione o svolgimento di funzioni ritenute fondamentali ai fini della sicurezza. L’elenco delle categorie individuato sulla base dei suddetti criteri è definito con il DPCM di cui all’articolo 1, comma 6, lettera a) da emanarsi nei termini previsti dal decreto- legge.

Il CAPO IV “Ispezioni e verifiche” si compone di sette articoli, dall’articolo 14 all’articolo 20.

**L’articolo 14 “Oggetto delle verifiche e delle ispezioni”** precisa che lo scopo delle verifiche e ispezioni, nell’ambito di applicazione del presente decreto, è di accertare l’adempimento da parte dei soggetti inclusi nel perimetro, degli obblighi previsti dal decreto-legge. A tal fine vengono quindi elencati tali obblighi che riguardano:

* la predisposizione, l’aggiornamento e la trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici;
* la notifica allo CSIRT (Computer Security Incident Response Team) Italiano degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici;
* l’adozione delle misure di sicurezza;
* la comunicazione al CVCN;
* l’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;
* la collaborazione per l'effettuazione delle attività di test da parte dei soggetti;
* l’osservanza delle prescrizioni formulate dalle Autorità competenti;
* l’osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto.

**L’articolo 15 “Autorità competenti”** definisce le Autorità competenti che possono effettuare le verifiche e le ispezioni. In particolare, si precisa che per la PCM la struttura preposta è quella competente per l’innovazione tecnologica e la digitalizzazione. Per il MiSE si precisa che la struttura preposta è quella competente in materia di tecnologie delle comunicazioni e di sicurezza informatica. L’articolo inoltre evidenzia che le Autorità competenti istituiscono un elenco del personale incaricato, il quale, ove necessario, deve essere in possesso della abilitazione di cui al regolamento adottato con del decreto del Presidente del Consiglio dei ministri 6 novembre 2015, n. 5. Le Autorità nominano sia il personale incaricato delle verifiche e ispezioni che il responsabile del procedimento. Il personale incaricato deve dichiarare di non trovarsi in conflitto di interessi. Infine, l’articolo prevede la possibilità che le Autorità si raccordino con le Autorità di settore di cui al decreto legislativo 18 maggio 2018, n.65 che recepisce la Direttiva europea NIS, anche al fine di avvalersi di personale dipendente esperto nei settori di cui al medesimo decreto legislativo.

**L’articolo 16 “Attività di verifica e ispezione”** elenca i casi nei quali le Autorità competenti possono effettuare verifiche e ispezioni ossia sulla base di atti di programmazione, notifiche di incidenti, rilevate difformità rispetto agli obblighi imposti dal decreto-legge e dai relativi decreti attuativi, segnalazioni provenienti da altre Autorità Pubbliche. L’articolo specifica che le ispezioni sono svolte dopo le verifiche e in base all’esito delle verifiche stesse, per trovare riscontri o per eventuali approfondimenti. Il responsabile del procedimento deve comunicare 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. I soggetti inclusi nel perimetro nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per le attività di verifica e ispezione, comunicandone il nominativo al responsabile del procedimento. L’articolo si conclude con l’indicazione della durata dei procedimenti. Il procedimento di verifica dura 90 giorni dal ricevimento delle evidenze richieste ai soggetti inclusi nel perimetro e il procedimento di ispezione dura 60 giorni dalla data di avvio delle attività ispettive presso le sedi utilizzate dai soggetti inclusi nel perimetro.

**L’articolo 17 “Attività di verifica”** descrive le modalità con cui sono effettuate le 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. Qualora l’Autorità lo ritenga opportuno, può chiedere tramite il responsabile del procedimento, informazioni e produzione di evidenze, quali ad esempio ulteriore documentazione, al responsabile della sicurezza. Si fa presente infatti che tra gli obblighi previsti c’è quello di detenzione di specifica documentazione. Entro 30 giorni dalla ricezione della richiesta, l’incaricato di cui all’articolo 16, comma 4, deve rendere disponibile quanto richiesto, secondo le modalità indicate nella richiesta. Qualora tali informazioni o documentazione, risultino incomplete o incongruenti, il responsabile del procedimento può richiedere chiarimenti e integrazioni ed entro 15 giorni dalla ricezione della richiesta, il soggetto deve fornire quanto richiesto, secondo le modalità indicate. Dell’attività svolta nel corso delle verifiche è redatto apposito verbale che il personale incaricato trasmette al responsabile del procedimento.

**L’articolo 18 “Attività di ispezione”** descrive le modalità con cui sono effettuate le attività di ispezione.

Le ispezioni si articolano nelle seguenti attività:

- riscontro delle evidenze acquisite ove le stesse presentino elementi meritevoli di approfondimento;

- analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari;

- esame dei chiarimenti richiesti ai sensi dell’articolo 17, comma 3.

Per lo svolgimento delle attività di ispezione, il personale incaricato può richiedere o eventualmente acquisire tutte le evidenze ritenute utili ai fini dell’accertamento. Le ispezioni possono essere effettuate presso le sedi utilizzate dai soggetti inclusi nel perimetro. L’intenzione di effettuare un’ispezione è comunicata dal responsabile del procedimento ai soggetti con un preavviso non inferiore a 15 giorni. La comunicazione riporta alcune informazioni minimali, in particolare:

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.

Qualora il soggetto avesse difficoltà a far condurre l’ispezione nei giorni selezionati, ha la possibilità di proporre date alternative, sebbene con delle limitazioni. In particolare, entro 7 giorni dalla ricezione della comunicazione con le date delle ispezioni, 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. In tal caso l’Autorità competente può accettare la proposta di modifica delle date, inviando una comunicazione almeno 7 giorni prima della prima data prevista per l’ispezione, oppure può 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. In mancanza della proposta alternativa da parte del soggetto, le date delle ispezioni si intendono confermate. Almeno 7 giorni prima dell’ispezione prevista, il soggetto comunica il nominativo del responsabile alla sicurezza che sarà l’unico referente per lo svolgimento delle attività ispettive. 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 precedentemente ricevuta. Potrebbe verificarsi il caso in cui si acquisisca durante l’ispezione, una notevole mole di dati per le quali non ci sarebbe il tempo di esaminarle subito, per cui si prevede esplicitamente che, qualora durante il corso dell’ispezione emergano evidenze meritevoli di approfondimento, le stesse possono essere esaminate in una fase successiva. A conclusione dell’attività ispettiva è redatto un 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 soggetto e una è trasmessa al responsabile del procedimento. Infine si prevede il fatto che gli ispettori possano venire a conoscenza di evidenze rientranti nelle attribuzioni istituzionali di altre Amministrazioni, in tal caso, il personale 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.

**L’articolo 19 “Esiti delle attività di verifica e ispezione”** descrive la conclusione delle attività di verifica e ispezione. L’esito di tali attività è raccolto dall’Autorità competente, la quale 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.

**L’articolo 20 “Invarianza finanziaria”** contiene la previsione che 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.