LEGGI ED ALTRI ATTI NORMATIVI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. **81**.

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

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la 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, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica e, in particolare, l'articolo 1, comma 3;

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

Visto il decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale e, in particolare, l'articolo 29;

Visto il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo e, in particolare, l'articolo 7-*bis*;

Vista la legge 3 agosto 2007, n. 124, recante Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto;

Visto il decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;

Visto il regolamento adottato con decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2, recante l'ordinamento e l'organizzazione del DIS;

Visto il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, ai sensi dell'articolo 1, comma 2, del decreto-legge n. 105 del 2019, in materia di perimetro di sicurezza nazionale cibernetica;

Visto il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, recante direttiva concernente indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana n. 87 del 13 aprile 2017;

Visto il decreto del Presidente del Consiglio dei ministri 8 agosto 2019, recante disposizioni sull'organizzazione e il funzionamento del *Computer security incident response team* - CSIRT italiano, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana n. 262 dell'8 novembre 2019;

Visto il «*Framework* nazionale per la *cybersecurity* e la data *protection*», edizione 2019 (*Framework* nazionale), realizzato dal Centro di ricerca di *cyber intelligence and information security* (CIS) dell'Università Sapienza di Roma e dal *Cybersecurity national lab* del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorità garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza (DIS), quale strumento di supporto per le organizzazioni pubbliche e private in materia di strategie e processi volti alla protezione dei dati personali, con specifico riferimento alla sicurezza degli stessi a fronte di possibili attacchi informatici, e alla sicurezza *cyber*, nonché per il loro continuo monitoraggio;

Considerato di dover tenere conto degli *standard* definiti a livello internazionale e dell'Unione europea e di assumere, quale base di riferimento per l'individuazione delle misure corrispondenti agli ambiti di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge n. 105 del 2019, il *Framework* nazionale, adeguandolo allo specifico contesto operativo delineato dal perimetro di sicurezza nazionale cibernetica e, pertanto, di richiamare, per ciascuna misura individuata, il codice alfanumerico identificativo della relativa sottocategoria del *Framework* nazionale;

Udito il parere del Consiglio di Stato espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 1° dicembre 2020;

Acquisiti i pareri delle Commissioni I e IX riunite, IV e V della Camera dei deputati e delle Commissioni 1ª, 4ª e 5ª del Senato della Repubblica;

Sulla proposta del Comitato interministeriale per la sicurezza della Repubblica;

ADOTTA
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) soggetti inclusi nel perimetro, i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge;

d) CISR, il Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124;

e) 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);

f) 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 n. 65 del 2018;

g) bene ICT (*information and communication technology*), un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge;

h) 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;

i) impatto sul bene ICT, limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali;

l) DIS, il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri, di cui all'articolo 4 della legge n. 124 del 2007;

m) CISR tecnico, l'organismo tecnico di supporto al CISR, di cui all'articolo 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2, che definisce l'ordinamento e l'organizzazione del DIS;

n) CSIRT italiano, il *Computer security incident response team* istituito presso il DIS ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018;

o) indicatori di compromissione (IOC), indicatori tecnici impiegati per la rilevazione di una minaccia o compromissione nota e generalmente riconducibili a indirizzi IP, elementi identificativi e moduli *software* afferenti agli strumenti tecnici impiegati da attori malevoli.

Capo II

NOTIFICHE DI INCIDENTE

Art. 2.

Tassonomia degli incidenti

1. Nelle tabelle n. 1 e n. 2 dell'allegato A al presente regolamento sono classificati, in categorie, gli incidenti aventi impatto sui beni ICT. Nella tabella n. 1 sono indicati gli incidenti meno gravi e nella tabella n. 2 quelli più gravi. Tale classificazione è funzionale alla diversa tempistica necessaria per una risposta efficace.

2. Nelle tabelle di cui al comma 1, per ciascuna tipologia di incidente, sono indicati un codice identificativo e la corrispondente categoria, accompagnata dalla descrizione di ciascuna tipologia di incidente.

Art. 3.

Notifica degli incidenti aventi impatto su beni ICT

1. Dal 1° gennaio 2022, i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A, procedono alla notifica al CSIRT italiano secondo le modalità di cui al presente regolamento.

2. Dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente a quella di entrata in vigore del presente regolamento, da quest'ultima data, e sino al 31 dicembre 2021, i soggetti inclusi nel perimetro procedono, in via sperimentale, alle notifiche di cui al comma 1, secondo le modalità di cui al comma 4.

3. I soggetti inclusi nel perimetro procedono alla notifica di cui ai commi 1 e 2 anche nei casi in cui uno degli incidenti individuati nelle tabelle di cui all'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'articolo 7, comma 2, del DPCM n. 131 del 2020, condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero *software* di base, quali sistemi operativi e di virtualizzazione.

4. I soggetti inclusi nel perimetro effettuano la notifica di cui ai commi 1, 2 e 3 entro sei ore, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A, ed entro un'ora, qualora si tratti di un incidente individuato nella tabella 2 del medesimo allegato. I predetti termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza, a seguito delle evidenze ottenute, anche mediante le attività di monitoraggio, test e controllo di cui all'articolo 1, comma 3, lettera *b)*,

numero 6, del decreto-legge, effettuate sulla base delle misure di sicurezza di cui all'allegato B, di un incidente riconducibile a una delle tipologie individuate nell'allegato A. La notifica è effettuata tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera *a)*, dell'allegato I, del decreto legislativo n. 65 del 2018, e secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

5. Qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi, tra cui le specifiche vulnerabilità sfruttate, la rilevazione di eventi comunque correlati all'incidente oggetto di notifica, ovvero gli indicatori di compromissione (IOC) rilevati, la notifica di cui al comma 1 è integrata tempestivamente dal momento in cui il soggetto incluso nel perimetro ne è venuto a conoscenza, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

6. Dal 1° gennaio 2022, i soggetti di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018, con la notifica di cui al presente articolo comunicano che la stessa, ai sensi dell'articolo 1, comma 8, lettera *b)*, del decreto-legge, costituisce anche adempimento dell'obbligo di notifica di cui, rispettivamente, agli articoli 12, comma 5, indicando a tal fine l'autorità competente NIS di cui all'articolo 7 del decreto legislativo n. 65 del 2018 alla quale la notifica deve essere inoltrata, e 14, comma 4, del decreto legislativo n. 65 del 2018. I soggetti di cui all'articolo 16-*ter*, comma 2, del decreto legislativo n. 259 del 2003, con la notifica di cui al presente articolo, comunicano che la stessa, ai sensi dell'articolo 1, comma 8, lettera *b)*, del decreto-legge, costituisce anche adempimento dell'obbligo previsto ai sensi dell'articolo 16-*ter* del decreto legislativo n. 259 del 2003 e delle correlate disposizioni attuative. Restano fermi, per le notifiche degli incidenti non rientranti nell'ambito di applicazione del decreto-legge, gli obblighi e le procedure di notifica previsti dal decreto legislativo n. 65 del 2018 e dal decreto legislativo n. 259 del 2003.

7. Su richiesta del CSIRT italiano, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1, 2 e 3 provvede, tramite i canali di comunicazione di cui al comma 4 ed entro sei ore dalla richiesta, a effettuare un aggiornamento della notifica, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

8. Una volta definiti e avviati i piani di attuazione delle attività per il ripristino dei beni ICT impattati dall'incidente oggetto di notifica, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1, 2 e 3, tramite i canali di comunicazione di cui al comma 4, ne dà tempestiva comunicazione al CSIRT italiano e trasmette, altresì, su richiesta del CSIRT italiano ed entro trenta giorni dalla stessa richiesta, una relazione tecnica che illustra gli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

9. I soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui alla sottocategoria 2.1.4 (ID.AM-6) dell'allegato B, ed in particolare all'incaricato e al referente tecnico di cui alla medesima sottocategoria.

10. Sino al 31 dicembre 2021, restano fermi per i soggetti inclusi nel perimetro, che effettuano, ai sensi del comma 2, le notifiche in via sperimentale, gli obblighi di notifica di cui agli articoli 12, comma 5, e 14, comma 4, del decreto legislativo n. 65 del 2018, nonché quelli previsti ai sensi dell'articolo 16-*ter* del decreto legislativo n. 259 del 2003 e delle correlate disposizioni attuative.

Art. 4.

Notifica volontaria degli incidenti

1. Al di fuori dei casi di cui all'articolo 3, i soggetti inclusi nel perimetro possono notificare, su base volontaria, gli incidenti, relativi ai beni ICT, non indicati nelle tabelle di cui all'allegato A, ovvero gli incidenti, indicati nelle tabelle di cui all'allegato A, relativi a reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai beni ICT. La notifica è effettuata tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera *a)*, dell'allegato I, del decreto legislativo n. 65 del 2018, e secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

2. Le notifiche volontarie sono trattate dal CSIRT italiano in subordine a quelle obbligatorie e qualora tale trattamento non costituisca un onere sproporzionato o eccessivo.

3. La notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

4. I soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui alla sottocategoria 2.1.4 (ID.AM-6) dell'allegato B, ed in particolare all'incaricato e al referente tecnico di cui alla medesima sottocategoria.

Art. 5.

Trasmissione delle notifiche

1. Il DIS inoltra le notifiche ricevute dal CSIRT italiano:

a) all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;

b) alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, qualora le notifiche provengano da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, fatta eccezione per quelle concernenti i beni ICT in relazione ai quali per le attività di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera *c)*, terzo periodo, del decreto-legge;

c) al Ministero dello sviluppo economico, qualora le notifiche provengano da un soggetto privato.

2. Le notifiche volontarie, di cui all'articolo 4, sono trasmesse solo nel caso in cui siano state trattate.

3. Il CSIRT italiano, ai sensi dell'articolo 1, comma 8, lettera *b)*, del decreto-legge, inoltra le notifiche ricevute dai soggetti inclusi nel perimetro, che siano identificati anche quali soggetti di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018, all'autorità competente NIS indicata ai sensi dell'articolo 3, comma 5.

4. Le modalità di inoltro delle notifiche previste ai commi 1 e 2 possono essere concordate mediante apposite intese con ciascuna delle amministrazioni interessate e, tenuto anche conto di quanto previsto dall'articolo 8, comma 4, con il Ministero della difesa.

Art. 6.

Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate

1. In materia di notifica degli incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

Capo III

MISURE DI SICUREZZA

Art. 7.

Misure di sicurezza

1. Le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere, sono individuate nell'allegato B al presente regolamento. La corrispondenza tra le misure di sicurezza e gli ambiti elencati all'articolo 1, comma 3, lettera *b)*, del decreto-legge, è indicata nella tabella in appendice n. 1 dell'allegato B. Nella tabella in appendice n. 2 del medesimo allegato B è indicata per ciascuna misura di sicurezza la corrispondente categoria di cui all'articolo 8, comma 1, lettera *a)*, ovvero lettera *b)*.

Art. 8.

Modalità e termini di adozione delle misure di sicurezza

1. I soggetti inclusi nel perimetro adottano, per ciascun bene ICT di rispettiva pertinenza, le misure di sicurezza di cui all'allegato B nei seguenti termini:

a) per le misure di sicurezza appartenenti alla categoria A di cui all'appendice n. 2 dell'allegato B, entro sei mesi dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente a quella di entrata in vigore del presente regolamento, entro sei mesi da quest'ultima data;

b) per le misure di sicurezza appartenenti alla categoria B di cui all'appendice n. 2 dell'allegato B, entro trenta mesi dalla data di trasmissione degli elenchi dei beni ICT effettuata ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, ovvero, qualora la trasmissione sia avvenuta in una data antecedente a quella di entrata in vigore del presente regolamento, entro trenta mesi da quest'ultima data.

2. I soggetti di cui al comma 1, dopo l'avvenuta adozione delle misure di sicurezza di cui all'allegato B, ne danno tempestivamente comunicazione al DIS, descrivendo le relative modalità, mediante la piattaforma digitale costituita presso il DIS ai sensi dell'articolo 9, comma 1, del regolamento adottato con DPCM n. 131 del 2020.

3. Ai fini della comunicazione di cui al comma 2, il DIS predispone un apposito modello di cui dà informazione ai soggetti di cui al comma 1.

4. Qualora un soggetto incluso nel perimetro proceda, ai sensi degli articoli 7 e 9 del regolamento adottato con

il DPCM n. 131 del 2020, all'aggiornamento dell'elenco dei beni ICT, valuta contestualmente se è necessario procedere all'adeguamento delle misure di sicurezza adottate ai sensi del presente articolo. Nel caso in cui sia necessario procedere all'adeguamento, vi provvede e ne comunica le relative modalità, con il modello di cui al comma 1, nei seguenti termini:

a) per le misure di sicurezza di cui alla categoria A dell'appendice n. 2 dell'allegato B, entro sei mesi dall'aggiornamento dell'elenco dei beni ICT;

b) per le misure di sicurezza di cui alla categoria B dell'appendice n. 2 dell'allegato B, entro trenta mesi dall'aggiornamento dell'elenco dei beni ICT.

5. In ogni altro caso in cui un soggetto incluso nel perimetro abbia proceduto ad adeguare le misure di sicurezza adottate ai sensi del presente articolo, ne comunica, entro sei mesi, le relative modalità con il modello di cui al comma 1.

6. Il DIS rende tempestivamente disponibili le comunicazioni ricevute ai sensi dei commi 1, 2 e 3 alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico ai fini dello svolgimento delle rispettive attività di verifica e ispezione, fatta eccezione per quelle comunicazioni concernenti i beni ICT in relazione ai quali per le attività di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera *c)*, terzo periodo, del decreto-legge.

Art. 9.

Tutela delle informazioni

1. Le misure minime di sicurezza individuate nell'allegato C al presente regolamento, e corrispondenti agli ambiti di cui all'articolo 1, comma 3, lettera *b)*, numeri 3 e 4, del decreto-legge, si applicano alle informazioni relative:

a) all'elencazione dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge;

b) agli elenchi di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, comprensivi della descrizione dell'architettura e della componentistica, nonché dell'analisi del rischio;

c) agli elementi delle notifiche effettuate ai sensi dell'articolo 3, ivi compresa la relazione di cui all'articolo 3, comma 7;

d) al modello di cui all'articolo 8, comma 1, e alla documentazione predisposta in attuazione delle misure di sicurezza di cui all'allegato B.

2. Le misure di sicurezza di cui all'allegato C si applicano entro sessanta giorni dalla data di entrata in vigore del presente regolamento.

3. Resta ferma l'adozione, da parte dei soggetti inclusi nel perimetro, delle misure di sicurezza di livello più elevato di cui all'allegato B, entro i termini indicati dall'articolo 8.

4. In caso di attribuzione alle informazioni di cui al comma 1 di una classifica di segretezza, ai sensi dell'articolo 42 della legge n. 124 del 2007, si applicano le misure di sicurezza previste dalla normativa vigente in materia.

Art. 10.

Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate

1. In materia di misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

Capo IV

DISPOSIZIONI FINALI

Art. 11.

Disposizioni finali

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

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

Roma, 14 aprile 2021

Il Presidente: DRAGHI

Visto, *il Guardasigilli:* CARTABIA

Registrato alla Corte dei conti il 4 giugno 2021
Ufficio di controllo sugli atti della Presidenza del Consiglio, del Ministero della giustizia e del Ministero degli affari esteri, registrazione n. 1450

Allegato A

(articolo 2)

Tassonomia degli incidenti

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

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

TABELLA 2

Identificativo	Categoria	Descrizione
ICP-B-1	**Azioni sugli obiettivi (*Actions on objectives*)**	**Inibizione delle funzioni di risposta (*Inhibit Response Function*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "*quality assurance*" dei sistemi di controllo industriale predisposte per rispondere a un disservizio o a uno stato anomalo.
ICP-B-2		**Compromissione dei processi di controllo (*Impair Process Control*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale.
ICP-B-3		**Disservizio intenzionale (*Impact*).** Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati. In tale ambito rientrano ad esempio gli eventi di tipo *Denial of Service*/*Distributed Denial of Service* che hanno impatto sui beni ICT.
ICP-B-4	**Disservizio (*Failure*)**	Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto nelle misure di sicurezza di cui all'allegato B, specie in termini di disponibilità, del bene ICT.
ICP-B-5		Divulgazione di dati corrotti o esecuzione operazioni corrotte tramite il bene ICT.
ICP-B-6		Divulgazione non autorizzata di dati digitali relativi ai beni ICT.

Allegato B

(*articolo 7*)

Misure di Sicurezza

1. PREMESSA

1. Il presente allegato definisce misure volte a garantire elevati livelli di sicurezza dei beni ICT ai sensi dell'articolo 1, comma 3, lettera *b)*, del decreto-legge, organizzate in funzioni, categorie e sottocategorie, ognuna identificata anche da un codice univoco alfanumerico corrispondente alle analoghe misure del *Framework* nazionale per la *cybersecurity* e la *data protection*", edizione 2019. Sono, altresì, indicate raccomandazioni, la cui attuazione è demandata alle valutazioni di ciascun soggetto incluso nel perimetro.
2. Per ogni misura è fornita una specifica più dettagliata dell'implementazione minima attesa, nonché delle modalità richieste al fine di descriverne l'adozione e dimostrarne l'attuazione.
3. Ad eccezione dell'organizzazione di *cybersecurity*, il termine "organizzazione", che compare all'interno delle descrizioni delle categorie e sottocategorie, è da intendersi riferito almeno ai beni ICT e al personale ad essi riconducibili a diverso titolo (utenti, amministratori, etc.).
4. Per ragioni di coerenza con i titoli delle categorie e sottocategorie del *Framework* nazionale è stato mantenuto il termine *cybersecurity* che, nell'ambito del presente allegato, è da intendersi equivalente alla locuzione "sicurezza cibernetica".
5. Ai fini del presente allegato, si intende per:
   a. **DPCM 1**, il decreto del Presidente del Consiglio dei ministri adottato ai sensi dell'articolo 1, comma 2, del decreto-legge n. 105 del 2019;
   b. **DPCM 2**, il decreto del Presidente del Consiglio dei ministri adottato ai sensi dell'articolo 1, comma 3, del decreto-legge n. 105 del 2019;
   c. **dipendenza esterna**, le reti, i sistemi informativi, i servizi informatici, le infrastrutture fisiche o gli altri servizi, ivi compresi quelli utilizzati per fini di manutenzione e gestione, di pertinenza di altri soggetti, da cui, in relazione agli esiti dell'analisi del rischio effettuata ai sensi dell'articolo 7, comma 2, del DPCM 1, dipende il funzionamento del bene ICT;
   d. **dipendenza interna**, le reti, i sistemi informativi, i servizi informatici, le infrastrutture fisiche o gli altri servizi, ivi compresi quelli utilizzati per fini di manutenzione e gestione, esterni al bene ICT, ma di pertinenza del soggetto, da cui, in relazione agli esiti dell'analisi del rischio effettuata ai sensi dell'articolo 7, comma 2, del DPCM 1, dipende il funzionamento del bene ICT;
   e. **modello di implementazione**, modello tramite il quale il soggetto comunica l'avvenuta adozione e le relative modalità di implementazione delle misure di sicurezza ai sensi del DPCM 2;
   f. **modello dei beni ICT**, modello tramite il quale il soggetto descrive l'architettura e la componentistica del bene ICT ai sensi dell'articolo 8 del DPCM 1;
   g. **catena di approvvigionamento *cyber***, la catena di approvvigionamento relativa a ciascun bene ICT.

2. IDENTIFICAZIONE (IDENTIFY)

2.1 Gestione degli asset (Asset Management) (ID.AM): I dati, il personale, i dispositivi e i sistemi e le *facility* necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.

2.1.1 ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione

1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto. L'elenco contiene, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT così come indicati nel modello dei beni ICT.
2. Tutti sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.

2.1.2 ID.AM-2: Sono censite le piattaforme e le applicazioni *software* in uso nell'organizzazione

1. Tutte le piattaforme e le applicazioni *software* installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto. L'elenco contiene, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT così come indicati nel modello dei beni ICT.
2. L'installazione delle piattaforme e delle applicazioni *software* è consentito esclusivamente per quelle approvate.
3. Si raccomanda, ove possibile e in relazione alla criticità delle piattaforme e delle applicazioni *software*, anche in esito all'analisi del rischio di cui al DPCM 1, che l'elenco di cui al punto 2 indichi degli identificatori univoci del codice oggetto installato e eseguito.

2.1.3 ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati

1. Tutti i flussi informativi tra il bene ICT e l'esterno del bene ICT, nonché tra il bene ICT e l'esterno del soggetto incluso nel perimetro sono identificati ed esiste un elenco dei flussi approvati da attori interni al soggetto. L'elenco contiene, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT così come indicati nell'modello dei beni ICT.

2.1.4 ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la *cybersecurity* per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, *partner*)

1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di *cybersecurity*, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. All'interno dell'organizzazione di cui al punto 1 è istituita e resa nota alle articolazioni competenti del soggetto l'articolazione per l'implementazione del perimetro.
3. È nominato, nell'ambito dell'articolazione di cui al punto 2, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del decreto-legge previste per i soggetti inclusi nel perimetro, in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto incluso nel perimetro ed assicura, almeno:

a. l'efficace implementazione delle misure di sicurezza di cui al DPCM 2;

b. la corretta esecuzione degli adempimenti relativi alla notifica degli incidenti aventi impatto su un bene ICT ai sensi dell'articolo 1, comma 3, lettera *a)*, del decreto-legge;

c. la collaborazione con il DIS, anche in relazione alle attività connesse all'articolo 5 del decreto-legge e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica (NSC), e con i soggetti incaricati dello svolgimento delle attività di verifica e ispezione di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge.

4. Sono nominati, nell'ambito dell'articolazione di cui al punto 2, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT italiano ai fini della gestione degli incidenti.
5. L'incaricato di cui al punto 3 e il referente tecnico di cui al punto 4 operano in stretto raccordo.
6. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 3 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto incluso nel perimetro al DIS, che li trasmette tempestivamente alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico per i profili di rispettiva competenza.
7. Esiste un elenco contenente tutto il personale interno e esterno impiegato nei processi di *cybersecurity* aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.
8. Esiste un elenco degli omologhi dell'incaricato di cui al punto 3 e del referente tecnico di cui al punto 4 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto incluso nel perimetro, in relazione alle dipendenze interne. L'elenco è disseminato presso le articolazioni competenti del soggetto incluso nel perimetro.

2.2 **Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di *cybersecurity*.

2.2.1 **ID.GV-1:** È identificata e resa nota una policy di *cybersecurity*

1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di *cybersecurity*. Il documento contiene anche il modello di implementazione.
2. Il modello di implementazione di cui al punto 1 è compilato e trasmesso secondo le modalità previste dal DPCM 2.

2.2.2 **ID.GV-4:** La governance ed i processi di risk management includono la gestione dei rischi legati alla *cybersecurity*

1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla *cybersecurity*.

2.3 Valutazione del rischio (Risk Assessment) (ID.RA): L'impresa comprende il rischio di *cybersecurity* inerente l'operatività dell'organizzazione (incluse la *mission*, le funzioni, l'immagine o la reputazione), gli *asset* e gli individui.

2.3.1 ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dei beni ICT e dell'efficacia delle misure di sicurezza tecniche e procedurali. Il piano contiene, inoltre, la periodicità e le modalità di esecuzione e, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT così come indicati nel modello dei beni ICT.
2. Le relazioni periodiche devono contenere almeno:
   a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse;
   b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza;
   c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità.

2.3.2 ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e i conseguenti impatti sono utilizzati per determinare il rischio

1. Questa misura implica l'analisi del rischio in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate.
2. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
3. Esiste un documento aggiornato di valutazione del rischio (*risk assessment*) che comprende almeno:
   a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento;
   b. qualora disponibili, le vulnerabilità emerse a seguito dell'esecuzione del piano di cui alla sottocategoria ID.RA-1 e a seguito dell'adozione delle misure di cui alla sottocategoria DE.CM-8;
   c. i potenziali impatti ritenuti significativi sui beni ICT, opportunamente descritti e valutati;
   d. l'identificazione, l'analisi e la ponderazione del rischio.

2.3.3 ID.RA-6: Sono identificate e prioritizzate le risposte al rischio

1. Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità.
2. Per il rischio residuo successivo al trattamento di cui al punto precedente esiste un documento aggiornato che ne contiene la chiara descrizione. Il documento, con il quale si accetta il rischio residuo, è approvato da parte dei vertici del soggetto.

2.4 Strategia della gestione del rischio (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.

2.4.1 ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente

1. Esiste un documento aggiornato di dettaglio che identifica e descrive il rischio tollerato dal soggetto.

2.5 Gestione del rischio relativo alla catena di approvvigionamento (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

2.5.1 ID.SC-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione

1. Esiste un documento aggiornato di dettaglio, che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

2.5.2 ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber

1. In merito all'affidamento di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), nonché di dipendenze esterne, di cui all'articolo 1, comma 6, del decreto-legge n. 105 del 2019, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, sono adottate misure in materia di sicurezza della catena di approvvigionamento attraverso:
   a. il coinvolgimento dell'organizzazione di *cybersecurity*, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione;
   b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore;
   c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del bene ICT;
   d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno:

1) della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza;

2) della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.

2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1. L'elenco contiene, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT ove si intendono impiegare i beni, sistemi e servizi, così come indicati nel modello dei beni ICT.

3. Si raccomanda, ove possibile e in relazione alla criticità della componente *software* (ivi incluso il *firmware*) dei beni e dei sistemi di *information and communication technology* (ICT), anche in esito all'analisi del rischio di cui al DPCM 1, di:

a. valutare l'affidabilità tecnica di cui al punto 1, lettera *d*, anche tenendo conto:

1) della disponibilità del fornitore a condividere il codice sorgente;

2) di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del *software* del produttore;

3) dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del *software* o *firmware* installato all'interno dei beni e dei sistemi di *information and communication technology*;

4) dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato e eseguito, con riferimento a quanto raccomandato al punto 3 della sottocategoria ID.AM-2.

b. adottare processi e strumenti tecnici per:

1) valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore;

2) acquisire il codice oggetto dai beni e sistemi di *information and communication technology*;

3) confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito, con riferimento a quanto raccomandato al punto 4 della sottocategoria ID.AM-2.

2.5.3 ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di *cybersecurity* dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento *cyber*

1. Le misure di sicurezza implementate dai terzi affidatari di servizi esterni sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al bene ICT. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.

2. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al bene ICT. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.

2.5.4 **ID.SC-4:** Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1. Esiste un documento aggiornato recante, almeno, le modalità e la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.
2. Esiste una pianificazione aggiornata degli audit, verifiche, o altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.

3. PROTEZIONE (PROTECT)

3.1 Gestione delle identità, autenticazione e controllo degli accessi (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate

3.1.1 PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza

1. Le credenziali di accesso sono individuali per gli utenti e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
2. Esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
3. Esiste una pianificazione aggiornata degli audit di sicurezza previsti e un registro degli audit di sicurezza effettuati con la relativa documentazione.

3.1.2 PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato

1. Con riferimento ai censimenti della categoria ID.AM-1, esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.1.3 PR.AC-3: L'accesso remoto alle risorse è amministrato

1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di *cybersecurity*.
2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzati degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.
3. Esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate;

b. l'elenco, con riferimento ai censimenti della categoria ID.AM e al modello di cui all'articolo 8 del DPCM 1, delle risorse a cui è possibile accedere da remoto e con quali modalità;

c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4. Esiste un log degli accessi da remoto eseguiti.

3.1.4 PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

1. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM, contiene almeno:

a. le risorse censite a cui è necessario accedere, con riferimento alla categoria ID.AM, per quali funzioni e con quali autorizzazioni;

b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni;

c. l'assegnazione degli utenti censiti ai gruppi di utenti.

3.1.5 PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

1. Con riferimento ai censimenti di cui alla categoria ID.AM, esiste un documento aggiornato di dettaglio contenente almeno:

a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti;

b. la descrizione delle reti segregate/segmentate;

c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza;

d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.

3.1.6 PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)

1. Esiste un documento aggiornato di dettaglio che, con riferimento ai censimenti di cui alla categoria ID.AM e alla valutazione del rischio di cui alla categoria ID.RA, contiene almeno:

a. le modalità di autenticazione disponibili;

b. la loro assegnazione alle categorie di transazioni.

3.2 Consapevolezza e addestramento (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti

3.2.1 PR.AT-1: Tutti gli utenti sono informati e addestrati

1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita agli utenti e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato, per ogni utente, di quali istruzioni ha ricevuto.

3.2.2 PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

1. Esiste un documento aggiornato di dettaglio, che indica i contenuti dell'istruzione fornita agli utenti con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un documento aggiornato recante, per ogni utente con privilegi, quali istruzioni ha ricevuto.

3.3 Sicurezza dei dati (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.

3.3.1 PR.DS-1: I dati memorizzati sono protetti

1. I dati digitali trattati mediante l'impiego di beni ICT, ivi compresi quelli relativi alla descrizione degli stessi beni, la cui compromissione sotto il profilo della disponibilità, integrità e riservatezza può avere impatto sullo svolgimento delle funzioni o dei servizi essenziali per i quali il soggetto è stato incluso nel perimetro, sono conservati, elaborati, ovvero estratti esclusivamente mediante l'impiego di infrastrutture fisiche e tecnologiche, anche se esternalizzate (ad esempio tramite *cloud computing*), localizzate sul territorio nazionale. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di *business continuity*.
2. I dati digitali utilizzati dalle infrastrutture deputate alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), nonché le infrastrutture di *disaster recovery*, anche se esternalizzate (ad esempio tramite *cloud computing*), devono essere localizzati sul territorio nazionale, salvo motivate e documentate ragioni di natura normativa o tecnica. In presenza di tali motivazioni i predetti dati e infrastrutture non devono comunque essere localizzati al di fuori del territorio dell'Unione europea.
3. Qualora opportunamente cifrati, i dati digitali di *backup*, anche se esternalizzati (ad esempio tramite *cloud computing*), possono essere conservati al di fuori del territorio nazionale, ma non al di fuori del territorio dell'Unione europea e le chiavi di cifratura devono essere comunque custodite all'interno del territorio nazionale. Le operazioni di cifratura e decifratura devono comunque essere eseguite mediante infrastrutture localizzate sul territorio nazionale.

4. Per i dati digitali e le infrastrutture di cui ai punti 2 e 3, ove localizzati al di fuori del territorio nazionale, l'applicazione delle misure ID.RA-5 e ID.RA-6 deve tenere opportunamente conto della localizzazione estera.
5. Le disposizioni di cui al punto 1, 2, 3 e 4 non si applicano alle sedi diplomatiche o consolari.
6. Esiste un documento aggiornato che descrive in quali sedi e infrastrutture sono conservati, elaborati ovvero estratti i dati digitali relativi ai beni ICT di cui ai punti 1, 2 e 3, ovvero le fattispecie di cui al punto 4.
7. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.3.2 PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.3.3 PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (*data leak*).

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per l'accesso ai dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.3.4 PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di *software*, *firmware* e delle informazioni

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di *software*, *firmware* e delle informazioni;
   b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.3.5 PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata;
   b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.4 Procedure e processi per la protezione delle informazioni (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del *management* e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset.

3.4.1 PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. *baseline*) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e di controllo industriale e il dispiegamento delle sole configurazioni adottate;
   b. l'elenco delle configurazioni dei sistemi IT e di controllo industriale impiegate e il riferimento alle relative pratiche di riferimento;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.4.2 PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni

1. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.4.3 PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per il *backup* delle informazioni;

b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.4.4 PR.IP-9: Sono attivi ed amministrati piani di risposta (*Incident Response* e *Business Continuity*) e recupero (*Incident Recovery* e *Disaster Recovery*) in caso di incidente/disastro

1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal bene ICT, e, se previsti, dalle *hot-replica* e/o *cold-replica* nonché dal sito(i) di *disaster recovery*, anche al fine di caratterizzare gli incidenti di cui all'articolo 1, comma 3, lettera a) del decreto-legge.
2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa/*disaster recovery*, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno:
   a. le politiche e i processi impiegati per identificare le priorità degli eventi;
   b. le fasi di attuazione dei piani;
   c. i ruoli e le responsabilità del personale;
   d. i flussi di comunicazione e reportistica;
   e. il raccordo con il CSIRT italiano.
3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.

3.4.5 PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità

1. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le politiche di sicurezza adottate per gestire le vulnerabilità;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3.5 Manutenzione (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.

3.5.1 PR.MA-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.

3. In base all'analisi del rischio, ogni aggiornamento dei *software* ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e il relativo codice oggetto dovrà essere custodito per almeno 24 mesi.

3.5.2 PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.
2. Tutti gli accessi eseguiti da remoto da personale di terze parti dovranno essere autorizzati dall'organizzazione di *cybersecurity* e limitati ai soli casi essenziali.
3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, dovranno essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.
6. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.

3.6 Tecnologie per la protezione (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

3.6.1 PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le politiche di sicurezza adottate per la gestione dei log dei sistemi;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.

3.6.2 PR.PT-4: Le reti di comunicazione e controllo sono protette

1. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, mantenuti e ben configurati.
2. Sistemi di prevenzione delle intrusioni (*intrusion prevention systems* - IPS) sono presenti, aggiornati, mantenuti e ben configurati.
3. Gli strumenti tecnici di cui ai punti 1 e 2 concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.

4. l'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1 e 2 sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA.
5. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE.
6. Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1, 2, 3 e 4.

3.6.3 PR.PT-5: Sono implementati meccanismi (es. *failsafe, load balancing, hot swap*) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse

1. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
   a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;
   b. esiste un sito di *disaster recovery*.
2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate.
3. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4. RILEVAMENTO (DETECT)

4.1 Anomalie e eventi (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

4.1.1 DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

1. Ai fini di rilevare tempestivamente incidenti con impatto soggetti alla notifica obbligatoria, sono adottati gli strumenti tecnici e procedurali per:
   a. acquisire le informazioni da più sensori e sorgenti;
   b. ottenere tempestivamente eventi, occorsi a carico di dipendenze interne o esterne, con impatti, anche potenziali, sul bene ICT;
   c. ricevere e raccogliere informazioni inerenti alla sicurezza dei beni ICT rese note dal CSIRT italiano, da fonti interne o esterne al soggetto;
   d. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a), b) e c), per rilevare tempestivamente eventi di interesse.
2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a);
   b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a), b) e c);
   c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera d).
   d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.

4.2 Monitoraggio continuo per la sicurezza (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

4.2.1 DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

1. Sono presenti sistemi di rilevamento delle intrusioni (*intrusion detection systems* – IDS).
2. Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.

3. Gli strumenti tecnici di cui ai punti 1 e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.
4. Gli strumenti tecnici di cui ai punti 1 e 2 sono impiegati anche per i fini di cui alla funzione DE.
5. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4.2.2 DE.CM-4: Il codice malevolo viene rilevato

1. Sistemi di protezione delle postazioni terminali (*endpoint protection systems* - EPS) e *antimalware* sono presenti.
2. I file in ingresso (tramite posta elettronica, *download*, dispositivi removibili, etc.) sono analizzati, anche tramite *sandbox*, prima di essere inseriti nel bene ICT.
3. Gli strumenti tecnici di cui ai punti 1 e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.
4. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 1, 2 e 3;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4.2.3 DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o *software* non autorizzati

1. Con riferimento alle sottocategorie PR.AC-2 e PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati.
2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete.
3. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei *software* non approvati.
4. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.
5. Gli strumenti tecnici di cui ai punti 1, 2, 3 e 4 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.
6. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 1, 2, 3 e 4;

b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

4.2.4 DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità

1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti *penetration test* e *vulnerability assessment*, prima della loro messa in esercizio.
2. Sono eseguiti periodicamente *penetration test* e *vulnerability assessment* in relazione alla criticità delle piattaforme e delle applicazioni *software*.
3. Esiste un documento aggiornato recante la tipologia di *penetration test* e *vulnerability assessment* previsti.
4. Esiste un registro aggiornato dei *penetration test* e *vulnerability assessment* eseguiti corredato dalla relativa documentazione.

4.3 Processi di rilevamento (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.

4.3.1 DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'*accountability*

1. Le nomine dell'incaricato e del referente di cui alla sottocategoria ID-AM-6 sono rese note all'interno del soggetto.
2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto e la successiva notifica al CSIRT italiano sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. i ruoli, i processi e le responsabilità di cui al punto 2;
   b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.

5. RISPOSTA (RESPOND)

5.1 Pianificazione della risposta (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

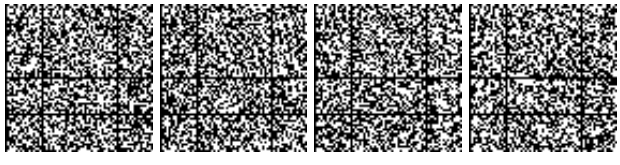
5.1.1 RS.RP-1: Esiste un piano di risposta (*response plan*) e questo viene eseguito durante o dopo un incidente

1. Esiste un piano di risposta aggiornato che prevede, almeno, l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE, nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica al CSIRT italiano degli incidenti con impatto sul bene ICT.
2. Il piano di risposta prevede anche le procedure per la mitigazione e risposta agli incidenti di cui all'articolo 1, comma 3, lettera a) del decreto-legge.

5.2 Comunicazione (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).

5.2.1 RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

1. Le fasi e i processi di gestione e risposta ad un incidente, incluse le relative interazioni con il CSIRT italiano, sono definite e rese note alle articolazioni competenti del soggetto.
2. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Sono eseguite periodicamente esercitazioni.
4. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le fasi, i processi, dei ruoli e le responsabilità di cui ai punti 1 e 2;
   b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2;
   c. le modalità per le esercitazioni di cui al punto 3.
5. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (*lesson learned*).



5.3 Analisi (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.

5.3.1 RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)

1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei *penetration test* e *vulnerability assessment* di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto e trasmessi al CSIRT italiano.
2. I canali di comunicazione del CSIRT italiano di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e *Information Sharing & Analysis Centre* (ISAAC) di riferimento sono monitorati.
3. Esiste un documento aggiornato che descrive, almeno:
   a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2;
   b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.

5.4 Mitigazione (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.

5.4.1 RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti

1. Viene implementato il piano di risposta di cui alla sottocategoria RS.RP-1 e gli esiti vengono riportati in un documento aggiornato anche ai fini dell'aggiornamento del citato piano di risposta.

5.4.2 RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.

6. RECUPERO (RECOVER)

6.1 Pianificazione del ripristino (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

6.1.1 RC.RP-1: Esiste un piano di ripristino (*recovery plan*) e viene eseguito durante o dopo un incidente di cybersecurity

1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento dei beni ICT coinvolti da un incidente di cybersecurity.
2. Il piano di ripristino prevede anche le procedure per il ripristino a seguito degli incidenti di cui all'articolo 1, comma 3, lettera a) del decreto-legge.

6.2 Miglioramenti (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "*lesson learned*" per le attività future.

6.2.1 RC.IM-2: Le strategie di recupero sono aggiornate

1. Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.

6.3 Comunicazione (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i *vendor*, i CERT/CSIRT).

6.3.1 RC.CO-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione

1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i *vendor*, i CERT/CSIRT), ivi incluse le articolazioni competenti del soggetto, anche ai fini dell'eventuale notifica al CSIRT italiano.

APPENDICE n. 1 - TABELLA DI CORRISPONDENZA (ambiti di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge)

Ambiti del decreto-legge ai sensi dell'articolo 1, comma 3, lettera b).	**Misure del presente allegato**
1) struttura organizzativa preposta alla gestione della sicurezza	2.1.4 ID.AM-6
	3.4.4 PR.IP-9, limitatamente al punto 2, lettera c
	4.3.1 DE.DP-1, limitatamente ai punti 1, 2 e 4, lettera a
	5.2.1 RS.CO-1, limitatamente ai punti 2 e 4
	5.3.1 RS.AN-5, limitatamente al punto 5
1-*bis*) politiche di sicurezza e gestione del rischio	2.2.1 ID.GV-1
	2.2.2 ID.GV-4
	2.3.1 ID.RA-1
	2.3.2 ID.RA-5
	2.3.3 ID.RA-6
	2.4.1 ID.RM-2
	2.5.1 ID.SC-1
	2.5.2 ID.SC-2
	2.5.3 ID.SC-3
	2.5.4 ID.SC-4
	3.1.1 PR.AC-1, limitatamente al punto 2
	3.1.2 PR.AC-2
	3.1.3 PR.AC-3, limitatamente al punto 3
	3.1.5 PR.AC-5
	3.3.1 PR.DS-1, limitatamente al punto 4
	3.3.2 PR.DS-3
	3.3.3 PS.DS-5
	3.3.4 PR.DS-6
	3.3.5 PR.DS-7
	3.4.1 PR.IP-1
	3.4.2 PR.IP-3
	3.4.3 PR.IP-4
	3.4.4 PR.IP-9, limitatamente al punto 2
	3.4.5 PR.IP-12
	3.5.1 PR.MA-1
	3.5.2 PR.MA-2
	3.6.1 PR.PT-1
	3.6.2 PR.PT-4, limitatamente ai punti 3, 4 e 6
	3.6.3 PR.PT-5, limitatamente al punto 3
	4.1.1 DE.AE-3, limitatamente al punto 2
	4.2.1 DE.CM-1, limitatamente ai punti 3 e 5
	4.2.2 DE.CM-4, limitatamente ai punti 3 e 5
	4.2.3 DE.CM-7, limitatamente ai punti 5 e 7

2) mitigazione e gestione degli incidenti e loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza	2.1.4 ID.AM-6, limitatamente al punto 4
	3.4.4 PR.IP-9
	5.1.1 RS.RP-1
	5.2.1 RS.CO-1
	5.3.1 RS.AN-5
	5.4.1 RS.MI-2
	5.4.2 RS.MI-3
	6.1.1 RC.RP-1
	6.2.1 RC.IM-2
	6.3.1 RC.CO-3
3) protezione fisica e logica dei dati	3.3.1 PR.DS-1
	3.3.2 PR.DS-3
	3.3.3 PR.DS-5
	3.3.4 PR.DS-6
	3.3.5 PR.DS-7
	3.4.3 PR.IP-4
4) integrità delle reti e dei sistemi informativi	2.1.1 ID.AM-1
	2.1.2 ID.AM-2
	2.1.3 ID.AM-3
	3.1.1 PR.AC-1
	3.1.2 PR.AC-2
	3.1.3 PR.AC-3
	3.1.4 PR.AC-4
	3.1.5 PR.AC-5
	3.1.6 PR.AC-7
	3.3.5 PR.DS-7
	3.4.1 PR.IP-1
	3.4.2 PR.IP-3
	3.4.3 PR.IP-4
	3.4.5 PR.IP-12
	3.5.2 PR.MA-2
5) gestione operativa, ivi compresa la continuità del servizio	3.4.4 PR.IP-9
	3.6.3 PR.PT-5
	6.1.1 RC.RP-1
	6.2.1 RC.IM-2
6) monitoraggio, test e controllo	2.3.1 ID.RA-1
	2.5.4 ID.SC-4
	3.1.1 PR.AC-1, limitatamente al punto 3
	3.1.3 PR.AC-3, limitatamente al punto 1
	3.5.1 PR.MA-1, limitatamente al punto 3
	3.6.2 PR.PT-4
	4.1.1 DE.AE-3
	4.2.1 DE.CM-1
	4.2.2 DE.CM-4
	4.2.3 DE.CM-7

	4.2.4 DE.CM-8
	4.3.1 DE.DP-1
7) formazione e consapevolezza	3.2.1 PR.AT-1
	3.2.2 PR.AT-2
	3.4.4 PR.IP-9, limitatamente ai punti 3 e 4
	5.2.1 RS.CO-1, limitatamente ai punti 3, 4 e 5
8) 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	2.1.4 ID.AM-6, limitatamente al punto 8
	2.5.1 ID.SC-1
	2.5.2 ID.SC-2
	2.5.3 ID.SC-3
	2.5.4 ID.SC-4

APPENDICE n. 2 - CATEGORIE (Tabella recante la ripartizione delle misure di sicurezza nelle categorie di cui all'art. 8, comma 1, lettere *a)* e *b)*)

Misure del presente allegato	Categorie di cui all'art. 8
2.1.1 ID.AM-1	A
2.1.2 ID.AM-2	B
2.1.3 ID.AM-3	A
2.1.4 ID.AM-6	A
2.2.1 ID.GV-1	A
2.2.2 ID.GV-4	A
2.3.1 ID.RA-1	A
2.3.2 ID.RA-5	A
2.3.3 ID.RA-6	B
2.4.1 ID.RM-2	A
2.5.1 ID.SC-1	A
2.5.2 ID.SC-2	B
2.5.3 ID.SC-3	B
2.5.4 ID.SC-4	A
3.1.1 PR.AC-1	B
3.1.2 PR.AC-2	B
3.1.3 PR.AC-3	B
3.1.4 PR.AC-4	B
3.1.5 PR.AC-5	B
3.1.6 PR.AC-7	B
3.2.1 PR.AT-1	A
3.2.2 PR.AT-2	A
3.3.1 PR.DS-1	B
3.3.2 PR.DS-3	A
3.3.3 PR.DS-5	B
3.3.4 PR.DS-6	B
3.3.5 PR.DS-7	B
3.4.1 PR.IP-1	B
3.4.2 PR.IP-3	B
3.4.3 PR.IP-4	B
3.4.4 PR.IP-9	A
3.4.5 PR.IP-12	A
3.5.1 PR.MA-1	B
3.5.2 PR.MA-2	B
3.6.1 PR.PT-1	B
3.6.2 PR.PT-4	B
3.6.3 PR.PT-5	B
4.1.1 DE.AE-3	B

4.2.1 DE.CM-1	B
4.2.2 DE.CM-4	B
4.2.3 DE.CM-7	B
4.2.4 DE.CM-8	B
4.3.1 DE.DP-1	A
5.1.1 RS.RP-1	A
5.2.1 RS.CO-1	A
5.3.1 RS.AN-5	A
5.4.1 RS.MI-2	A
5.4.2 RS.MI-3	B
6.1.1 RC.RP-1	A
6.2.1 RC.IM-2	A
6.3.1 RC.CO-3	A

Allegato C

(*articolo 9*)

Misure minime di sicurezza per la tutela delle informazioni

1. Trattamenti con l'ausilio di strumenti elettronici

a) Identificazione degli utenti e gestione delle identità digitali;

b) determinazione dei privilegi di accesso alle risorse da associare agli utenti e agli addetti o incaricati alla gestione o alla manutenzione;

c) implementazione di un sistema di autenticazione e autorizzazione degli utenti secondo i privilegi individuati al punto precedente;

d) protezione contro il software malevolo mediante l'impiego di *software antimalware* aggiornato

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) procedure di sicurezza per l'importazione e l'esportazione dei dati sui sistemi impiegati;

g) procedure per la gestione della configurazione dei sistemi impiegati;

h) procedure per la dismissione dei dispositivi di memorizzazione utilizzati sui sistemi impiegati;

i) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

l) adozione di tecniche di cifratura.

2. Misure di sicurezza fisica e documentale

a) L'accesso alle informazioni è consentito sulla base del principio della necessità di conoscere (*need to know*);

b) deve essere individuata la figura di un responsabile incaricato della gestione delle informazioni, preferibilmente già in possesso di abilitazione di sicurezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124;

c) la documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedura di tracciamento delle chiavi in uso;

d) la documentazione deve essere registrata su appositi registri di protocollo;

e) la consultazione dei documenti deve avvenire sulla base del principio della necessità di conoscere (*need to know*) e deve essere tracciata su apposito registro;

f) la riproduzione dei documenti può avvenire solo previa autorizzazione del responsabile della gestione delle informazioni e deve essere registrata su apposito registro;

g) la documentazione deve essere spedita tramite corrieri.

N O T E

AVVERTENZA:

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

Note alle premesse:

— La legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri), è pubblicata nella *Gazzetta Ufficiale* 12 settembre 1988, n. 214, S.O. n. 86.

— Si riporta il testo del comma 3 dell'articolo 1 del decreto-legge 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), pubblicato nella *Gazzetta Ufficiale* 21 settembre 2019, n. 222, convertito , con modificazioni, dalla legge 18 novembre 2019, n. 133, pubblicata nella *Gazzetta Ufficiale* 20 novembre 2019, n. 272:

«Art. 1. *(Perimetro di sicurezza nazionale cibernetica)*. — 1. – 2. (*Omissis*).

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

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

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

1) alla struttura organizzativa preposta alla gestione della sicurezza;

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

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

3) alla protezione fisica e logica e dei dati;

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

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

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

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

4. – 19-*ter*. (*Omissis*).».

— Il decreto legislativo 30 luglio 1999, n. 300 (Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59), è pubblicato nella *Gazzetta Ufficiale* 30 agosto 1999, n. 203, S.O. n. 163.

— Il decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche), è pubblicato nella *Gazzetta Ufficiale* 15 settembre 2003, n. 214, S.O. n. 150.

— Si riporta il testo dell'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), pubblicato nella *Gazzetta Ufficiale* 16 maggio 2005, n. 112, S.O. n. 93:

«Art. 29. *(Qualificazione dei fornitori di servizi)*. — 1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida.

2. Ai fini della qualificazione, i soggetti di cui al comma 1 devono possedere i requisiti di cui all'articolo 24 del regolamento (UE) 23 luglio 2014, n. 910/2014, disporre di requisiti di onorabilità, affidabilità, tecnologici e organizzativi compatibili con la disciplina europea, nonché di garanzie assicurative adeguate rispetto all'attività svolta. Con decreto del Presidente del Consiglio dei ministri, o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, sentita l'AgID, nel rispetto della disciplina europea, sono definiti i predetti requisiti in relazione alla specifica attività che i soggetti di cui al comma 1 intendono svolgere. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche.

3.

4. La domanda di qualificazione si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità di AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto da AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. – 8.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse di AgID, senza nuovi o maggiori oneri per la finanza pubblica.».

— Si riporta il testo dell'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale), pubblicato nella *Gazzetta Ufficiale* 27 luglio 2005, n. 173, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, pubblicata nella *Gazzetta Ufficiale* 1° agosto 2005, n. 177:

«Art. 7-*bis*. *(Sicurezza telematica)*. — 1. Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n. 801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

2. Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, gli ufficiali di polizia giudiziaria appartenenti all'organo di cui al comma 1 possono svolgere le attività di cui all'articolo 4, commi 1 e 2, del decreto-legge 18 ottobre 2001, n. 374, convertito, con modificazioni, dalla legge 15 dicembre 2001, n. 438, e quelle di cui all' articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati.».

— La legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto), è pubblicata nella *Gazzetta Ufficiale* 13 agosto 2007, n.187.

— Il decreto legislativo 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione), è pubblicato nella *Gazzetta Ufficiale* 9 giugno 2018, n.132.

— Il comunicato relativo all'adozione del decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2 (Regolamento che definisce l'ordinamento e l'organizzazione del Dipartimento delle informazioni per la sicurezza (DIS)), è pubblicato nella *Gazzetta Ufficiale* 10 aprile 2020, n. 96.

— Il decreto del Presidente del Consiglio dei ministri 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), è pubblicato nella *Gazzetta Ufficiale* 21 ottobre 2020, n. 261.

— Il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali), è pubblicato nella *Gazzetta Ufficiale* 13 aprile 2017, n. 87.

— Il decreto del Presidente del Consiglio dei ministri 8 agosto 2019 (Disposizioni sull'organizzazione e il funzionamento del *Computer securty incident response team* - CSIRT italiano), è pubblicato nella *Gazzetta Ufficiale* 8 novembre 2019 n. 262.

Note all'art. 1:

— Si riporta il testo dei commi 1 e 2-*bis* dell'articolo 1, del citato decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

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

2. (*Omissis*).

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

3. – 19-*ter*. (*Omissis*).».

— Si riporta il testo dell'articolo 5 della citata legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto):

«Art. 5. *(Comitato interministeriale per la sicurezza della Repubblica)*. — 1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la sicurezza della Repubblica (CISR) con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza.

2.Il Comitato elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza, delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico e dal Ministro della transizione ecologica.

4. Il direttore generale del DIS svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, i direttori dell'AISE e dell'AISI, nonché altre autorità civili e militari di cui di volta in volta sia ritenuta necessaria la presenza in relazione alle questioni da trattare.».

— Si riporta il testo del comma 1, lettera *dd)* dell'articolo 1 del citato decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche):

«Art. 1. *(Definizioni)*. — 1. Ai fini del presente Codice si intende per:

a). – *cc)*. (*Omissis*);

dd) reti di comunicazione elettronica: i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

ee). – qq-*quater*). (*Omissis*).».

— Si riporta il testo del comma 1, lettera *aa)*, dell'articolo 3 del citato decreto legislativo 18 maggio 2018, n. 65:

«Art. 3. *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

a). – *zz)*. (*Omissis*);

aa) servizio di *cloud computing*, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.».

— Si riporta il testo dell'articolo 1, comma 2, lettera *b)* del citato decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1. *(Perimetro di sicurezza nazionale cibernetica)*. — 2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):

a). (*Omissis*);

b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al comma 2-*bis* trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico; la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.».

— Si riporta il testo dell'articolo 4, della citata legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto):

«Art. 4. *(Dipartimento delle informazioni per la sicurezza)*. — 1. Per lo svolgimento dei compiti di cui al comma 3 è istituito, presso la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni per la sicurezza (DIS).

2. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza.

3. Il DIS svolge i seguenti compiti:

a) coordina l'intera attività di informazione per la sicurezza, verificando altresì i risultati delle attività svolte dall'AISE e dall'AISI, ferma restando la competenza dei predetti servizi relativamente alle attività di ricerca informativa e di collaborazione con i servizi di sicurezza degli Stati esteri;

b) è costantemente informato delle operazioni di competenza dei servizi di informazione per la sicurezza e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema di informazione per la sicurezza;

c) raccoglie le informazioni, le analisi e i rapporti provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati; ferma l'esclusiva competenza dell'AISE e dell'AISI per l'elaborazione dei rispettivi piani di ricerca operativa, elabora analisi strategiche o relative a particolari situazioni; formula valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI;

d) elabora, anche sulla base delle informazioni e dei rapporti di cui alla lettera *c)*, analisi globali da sottoporre al CISR, nonché progetti di ricerca informativa, sui quali decide il Presidente del Consiglio dei ministri, dopo avere acquisito il parere del CISR;

d-*bis*) sulla base delle direttive di cui all'articolo 1, comma 3-*bis*, nonché delle informazioni e dei rapporti di cui alla lettera *c)* del presente comma, coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

e) promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia; comunica al Presidente del Consiglio dei ministri le acquisizioni provenienti dallo scambio informativo e i risultati delle riunioni periodiche;

f) trasmette, su disposizione del Presidente del Consiglio dei ministri, sentito il CISR, informazioni e analisi ad amministrazioni pubbliche o enti, anche ad ordinamento autonomo, interessati all'acquisizione di informazioni per la sicurezza;

g) elabora, d'intesa con l'AISE e l'AISI, il piano di acquisizione delle risorse umane e materiali e di ogni altra risorsa comunque strumentale all'attività dei servizi di informazione per la sicurezza, da sottoporre all'approvazione del Presidente del Consiglio dei ministri;

h) sentite l'AISE e l'AISI, elabora e sottopone all'approvazione del Presidente del Consiglio dei ministri lo schema del regolamento di cui all'articolo 21, comma 1;

i) esercita il controllo sull'AISE e sull'AISI, verificando la conformità delle attività di informazione per la sicurezza alle leggi e ai regolamenti, nonché alle direttive e alle disposizioni del Presidente del Consiglio dei ministri. Per tale finalità, presso il DIS è istituito un ufficio ispettivo le cui modalità di organizzazione e di funzionamento sono definite con il regolamento di cui al comma 7. Con le modalità previste da tale regolamento è approvato annualmente, previo parere del Comitato parlamentare di cui all'articolo 30, il piano annuale delle attività dell'ufficio ispettivo. L'ufficio ispettivo, nell'ambito delle competenze definite con il predetto regolamento, può svolgere, anche a richiesta del direttore generale del DIS, autorizzato dal Presidente del Consiglio dei ministri, inchieste interne su specifici episodi e comportamenti verificatisi nell'ambito dei servizi di informazione per la sicurezza;

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;

m) cura le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale;

n) impartisce gli indirizzi per la gestione unitaria del personale di cui all'articolo 21, secondo le modalità definite dal regolamento di cui al comma 1 del medesimo articolo;

n-*bis*) gestisce unitariamente, ferme restando le competenze operative dell'AISE e dell'AISI, gli approvvigionamenti e i servizi logistici comuni.

4. Fermo restando quanto previsto dall'articolo 118-*bis* del codice di procedura penale, introdotto dall'articolo 14 della presente legge, qualora le informazioni richieste alle Forze di polizia, ai sensi delle lettere *c)* ed *e)* del comma 3 del presente articolo, siano relative a indagini di polizia giudiziaria, le stesse, se coperte dal segreto di cui all'articolo 329 del codice di procedura penale, possono essere acquisite solo previo nulla osta della autorità giudiziaria competente. L'autorità giudiziaria può trasmettere gli atti e le informazioni anche di propria iniziativa.

5. La direzione generale del DIS è affidata ad un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al Presidente del Consiglio dei ministri, sentito il CISR. L'incarico ha comunque la durata massima di quattro anni ed è rinnovabile con successivi provvedimenti per una durata complessiva massima di ulteriori quattro anni. Per quanto previsto dalla presente legge, il direttore del DIS è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, salvo quanto previsto dall'articolo 6, comma 5, e dall'articolo 7, comma 5, ed è gerarchicamente e funzionalmente sovraordinato al personale del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento.

6. Il Presidente del Consiglio dei ministri, sentito il direttore generale del DIS, nomina uno o più vice direttori generali; il direttore generale affida gli altri incarichi nell'ambito del dipartimento, ad eccezione degli incarichi il cui conferimento spetta al Presidente del Consiglio dei ministri.

7. L'ordinamento e l'organizzazione del DIS e degli uffici istituiti nell'ambito del medesimo dipartimento sono disciplinati con apposito regolamento.

8. Il regolamento previsto dal comma 7 definisce le modalità di organizzazione e di funzionamento dell'ufficio ispettivo di cui al comma 3, lettera *i)*, secondo i seguenti criteri:

a) agli ispettori è garantita piena autonomia e indipendenza di giudizio nell'esercizio delle funzioni di controllo;

b) salva specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, i controlli non devono interferire con le operazioni in corso;

c) sono previste per gli ispettori specifiche prove selettive e un'adeguata formazione;

d) non è consentito il passaggio di personale dall'ufficio ispettivo ai servizi di informazione per la sicurezza;

e) gli ispettori, previa autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, possono accedere a tutti gli atti conservati presso i servizi di informazione per la sicurezza e presso il DIS; possono altresì acquisire, tramite il direttore generale del DIS, altre informazioni da enti pubblici e privati.».

— Per il comunicato relativo all'adozione del decreto del Presidente del Consiglio dei ministri 3 aprile 2020, n. 2 (Regolamento che definisce l'ordinamento e l'organizzazione del Dipartimento delle informazioni per la sicurezza (DIS)), si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 8, del citato decreto legislativo 18 maggio 2018, n. 65:

«Art. 8. *(Gruppi di intervento per la sicurezza informatica in caso di incidente – CSIRT)*. — 1. È istituito, presso la Presidenza del Consiglio dei ministri - Dipartimento delle informazioni per la sicurezza, il CSIRT italiano, che svolge i compiti e le funzioni del *Computer emergency response team* (CERT) nazionale, di cui all'articolo 16-*bis* del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

2. L'organizzazione e il funzionamento del CSIRT italiano sono disciplinati con decreto del Presidente del Consiglio dei ministri ai sensi dell'articolo 7 del decreto legislativo 30 luglio 1999, n. 303, da adottare entro il 9 novembre 2018.

3. Nelle more dell'adozione del decreto di cui al comma 2, le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro.

4. Il CSIRT italiano assicura la conformità ai requisiti di cui all'allegato I, punto 1, svolge i compiti di cui all'allegato I, punto 2, si occupa dei settori di cui all'allegato II e dei servizi di cui all'allegato III e dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale.

5. Il CSIRT italiano definisce le procedure per la prevenzione e la gestione degli incidenti informatici.

6. Il CSIRT italiano garantisce la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT di cui all'articolo 11.

7. La Presidenza del Consiglio dei ministri comunica alla Commissione europea il mandato del CSIRT italiano e le modalità di trattamento degli incidenti a questo affidati.

8. Il CSIRT italiano, per lo svolgimento delle proprie funzioni, può avvalersi anche dell'Agenzia per l'Italia digitale.

9. Le funzioni svolte dal Ministero dello sviluppo economico in qualità di CERT nazionale ai sensi dell'articolo 16-*bis*, del decreto le-

gislativo 1° agosto 2003, n. 259, nonché quelle svolte da Agenzia per l'Italia digitale in qualità di CERT-PA, ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, sono trasferite al CSIRT italiano a far data dalla entrata in vigore del decreto di cui al comma 2.

10. Per le spese relative al funzionamento del CSIRT italiano è autorizzata la spesa di 2.000.000 di euro annui a decorrere dall'anno 2020. A tali oneri si provvede ai sensi dell'articolo 22.».

Note all'art. 3:

— Si riporta il testo del comma 2 dell'articolo 7 del citato decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131:

«Art. 7. *(Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici)*. — 1. (*Omissis*).

2. Ricevuta la comunicazione prevista dall'articolo 1, comma 2-*bis*), secondo periodo, del decreto-legge, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale di cui all'articolo 4, comma 1, lettera *c)*, provvedono:

a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati:

1) l'impatto di un incidente sul bene ICT, 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;

2) 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 dei beni ICT di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge. In fase di prima applicazione e fino all'aggiornamento del presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, 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.

3. (*Omissis*).».

— Si riporta il testo del punto 1, lettera *a)*, dell'allegato I, del citato decreto legislativo 18 maggio 2018, n. 65:

«ALLEGATO I
Requisiti e compiti dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)

I requisiti e i compiti del CSIRT sono adeguatamente e chiaramente definiti ai sensi del presente decreto e del decreto del Presidente del Consiglio dei ministri di cui all'art. 8, comma 2. Essi includono quanto segue:

1. Requisiti per il CSIRT:

a) Il CSIRT garantisce un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano;

b). – d). (*Omissis*).».

— Si riporta il testo degli articoli 12 e 14 del citato decreto legislativo 18 maggio 2018, n. 65:

«Art. 12. *(Obblighi in materia di sicurezza e notifica degli incidenti)*. — 1. Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

2.Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.

3.Nell'adozione delle misure di cui ai commi 1 e 2, gli operatori di servizi essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione di cui all'articolo 10, nonché delle linee guida di cui al comma 7.

4. Fatto salvo quanto previsto dai commi 1, 2 e 3, le autorità competenti NIS possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali.

5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.

7. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare un eventuale impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente. Le autorità competenti NIS possono predisporre linee guida per la notifica degli incidenti.

8. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri:

a) il numero di utenti interessati dalla perturbazione del servizio essenziale;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente.

9. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, il CSIRT italiano informa gli eventuali altri Stati membri interessati in cui l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali.

10. Ai fini del comma 9, il CSIRT italiano preserva, conformemente al diritto dell'Unione europea e alla legislazione nazionale, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella notifica secondo quanto previsto dall'articolo 1, comma 5.

11. Ove le circostanze lo consentano, il CSIRT italiano fornisce all'operatore di servizi essenziali, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente.

12. Su richiesta dell'autorità competente NIS o del CSIRT italiano, il punto di contatto unico trasmette, previa verifica dei presupposti, le notifiche ai punti di contatto unici degli altri Stati membri interessati.

13. Previa valutazione da parte dell'organo di cui al comma 6, l'autorità competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato l'operatore dei servizi essenziali notificante, può informare il pubblico in merito ai singoli incidenti, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso.

14. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Gli operatori di servizi essenziali provvedono agli adempimenti previsti dal presente articolo a valere sulle risorse finanziarie disponibili sui propri bilanci.»

«Art. 14. (Obblighi in materia di sicurezza e notifica degli incidenti). — 1. I fornitori di servizi digitali identificano e adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione europea.

2. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi:

a) la sicurezza dei sistemi e degli impianti;

b) trattamento degli incidenti;

c) gestione della continuità operativa;

d) monitoraggio, audit e test;

e) conformità con le norme internazionali.

3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e

dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.

4. I fornitori di servizi digitali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.

5. Le notifiche includono le informazioni che consentono al CSIRT italiano di determinare la rilevanza di un eventuale impatto transfrontaliero. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo di cui all'articolo 12, comma 6.

7. Al fine di determinare la rilevanza dell'impatto di un incidente, sono tenuti in considerazione, in particolare, i seguenti parametri:

a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente;

d) la portata della perturbazione del funzionamento del servizio;

e) la portata dell'impatto sulle attività economiche e sociali.

8. L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente con riferimento ai parametri di cui al comma 7.

9. Qualora un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali, l'operatore stesso notifica qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di tale operatore.

10. Qualora l'incidente di cui al comma 4 riguardi due o più Stati membri, il CSIRT italiano informa gli altri Stati membri coinvolti.

11. Ai fini del comma 9, il CSIRT italiano tutela, nel rispetto del diritto dell'Unione europea e della legislazione nazionale, la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonché la riservatezza delle informazioni fornite.

12. Previa valutazione da parte dell'organo di cui all'articolo 12, comma 6, l'autorità competente NIS, d'intesa con il CSIRT italiano, dopo aver consultato il fornitore di servizi digitali interessato e, se del caso, le autorità competenti o i CSIRT degli altri Stati membri interessati, può informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestirne uno in corso, o qualora sussista comunque un interesse pubblico alla divulgazione dell'incidente.

13. I fornitori di servizi digitali applicano le disposizioni di attuazione degli atti di esecuzione della Commissione europea che specificano ulteriormente le misure tecnico-organizzative di cui al comma 1 e i parametri, ivi compresi formati e procedure, relativi agli obblighi di notifica di cui al comma 4.

14. Fatto salvo quanto previsto dall'articolo 1, comma 7, non sono imposti ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali.

15. Il presente capo non si applica alle microimprese e alle piccole imprese quali definite nella raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.».

— Si riporta il testo dell'articolo 1, comma 8, lettera *b)*, del citato decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1. *(Perimetro di sicurezza nazionale cibernetica)*. — 1. – 7. (*Omissis*).

8. I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-*ter*, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:

a) (*Omissis*);

b) assolvono l'obbligo di notifica di cui al comma 3, lettera *a)*, che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, e delle correlate disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera *a)*, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT italiano inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera *a)*, all'autorità competente di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.

9. – 19-*ter*. (*Omissis*).».

— Si riporta il testo dell'articolo 16-*ter*, del citato decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche):

«Art. 16-*ter (Attuazione e controllo)*. — 1. Le misure adottate ai fini dell'attuazione del presente articolo e dell'articolo 16-*bis* sono approvate con decreto del Ministro dello sviluppo economico.

2. Ai fini del controllo del rispetto dell'articolo 16-*bis* le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico sono tenute a:

a) fornire al Ministero, e se necessario all'Autorità, le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti, in particolare i documenti relativi alle politiche di sicurezza; nonché;

b) sottostare a una verifica della sicurezza effettuata dal Ministero, anche su impulso dell'Autorità, in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico, o da un organismo qualificato indipendente designato dal Ministero. L'impresa si assume l'onere finanziario della verifica.

3. Il Ministero e l'Autorità hanno la facoltà di indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza e l'integrità delle reti.

4. Nel caso in cui il Ministero riscontri, anche su indicazione dell'Autorità, il mancato rispetto degli articoli 16-*bis* o 16-*ter* ovvero delle disposizioni attuative previste dal comma 1 da parte delle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, si applicano le sanzioni di cui all'articolo 98, commi da 4 a 12.».

Note all'art. 5:

— Per il testo dell'articolo 7-*bis*, del decreto-legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale) convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, si veda nelle note alle premesse.

— Per il testo dell'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 1, comma 6, lettera *c)*, del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1. *(Perimetro di sicurezza nazionale cibernetica)*. — 1.-5- (*Omissis*).

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

a). – b). (*Omissis*);

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

oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.».

— Per il testo dell'articolo 1, comma 8, lettera *b)*, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, si veda nelle note all'articolo 3.

— Per il testo degli articoli 12 e 14 del citato decreto legislativo 18 maggio 2018, n. 65, si veda nelle note all'articolo 3.

Note all'art. 6:

— Per il testo dell'articolo 1, comma 2, lettera *b)* del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note all'articolo 1.

— Per il testo dell'articolo 4, comma 3, lettera *l)*, della citata legge n. 124 del 2007, si veda nelle note all'articolo 1.

Note all'art. 7:

— Per il testo dell'articolo 1, comma 3, lettera *b)*, numeri 3 e 4, del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note alle premesse.

Note all'art. 8:

— Si riporta il testo degli articoli 7 e 9 del citato decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131:

«Art. 7. *(Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici)*. — 1. Ai sensi dell'articolo 1, comma 2, del decreto-legge, i soggetti inclusi nel perimetro predispongono e aggiornano, con cadenza almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono, osservando i criteri individuati nel successivo comma.

2. Ricevuta la comunicazione prevista dall'articolo 1, comma 2-*bis*), secondo periodo, del decreto-legge, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale di cui all'articolo 4, comma 1, lettera *c)*, provvedono:

a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati:

1) l'impatto di un incidente sul bene ICT, 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;

2) 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 dei beni ICT di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge. In fase di prima applicazione e fino all'aggiornamento del presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, 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.

3. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate si applica quanto previsto dall'articolo 1, comma 2, lettera *b)*, del decreto-legge.»

«Art. 9. *(Modalità di trasmissione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici)*. — 1. Entro sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco di cui all'articolo 1, comma 2-*bis*), del decreto-legge, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, nonché quelli privati ivi inclusi, trasmettono, rispettivamente, alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico, gli elenchi di beni ICT di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, comprensivi della descrizione dell'architettura e della componentistica predisposta secondo il modello di cui all'articolo 8, nonché dell'analisi del rischio. 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 NSC, nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente. Le disposizioni di cui al presente comma si applicano anche per l'aggiornamento degli elenchi di beni ICT e del modello di cui all'articolo 8, comma 1.

2. 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 alla piattaforma di cui al comma 1 ai fini dello svolgimento delle attività di ispezione e verifica previste dall'articolo 1, comma 6, lettera *c)*, del decreto-legge, nonché dei compiti di cui all'articolo 1, comma 12, del decreto-legge.

3. 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 di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione accede alla piattaforma di cui al comma 1 limitatamente alle informazioni necessarie, individuate ai sensi dell'articolo 8, comma 2, per lo svolgimento dei compiti previsti dall'articolo 1, comma 12, del decreto-legge.

4. L'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, accede per il tramite della piattaforma digitale di cui al comma 1 agli elenchi di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, e fornisce alla stessa piattaforma gli elenchi di pertinenza del Ministero.».

— Per il testo dell'articolo 1, comma 2, lettera *b)* del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note all'articolo 1.

— Per il testo del punto 1, lettera *a)*, dell'allegato I, del citato decreto legislativo 18 maggio 2018, n. 65, si veda nelle note all'articolo 3.

— Per il testo dell'articolo 1, comma 6, lettera *c)*, del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note all'articolo 5.

Note all'art. 9:

— Per il testo dell'articolo 1, commi 2, 2-*bis* e 3, lettera *b)*, numeri 3 e 4, del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 42, della citata legge 3 agosto 2007, n. 124:

«Art. 42. *(Classifiche di segretezza)*. — 1. Le classifiche di segretezza sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali.

1-*bis*. Per la trattazione di informazioni classificate segretissimo, segreto e riservatissimo è necessario altresì il possesso del nulla osta di sicurezza (NOS).

2. La classifica di segretezza è apposta, e può essere elevata, dall'autorità che forma il documento, l'atto o acquisisce per prima la notizia, ovvero è responsabile della cosa, o acquisisce dall'estero documenti, atti, notizie o cose.

3. Le classifiche attribuibili sono: segretissimo, segreto, riservatissimo, riservato. Le classifiche sono attribuite sulla base dei criteri ordinariamente seguiti nelle relazioni internazionali.

4. Chi appone la classifica di segretezza individua, all'interno di ogni atto o documento, le parti che devono essere classificate e fissa specificamente il grado di classifica corrispondente ad ogni singola parte.

5. La classifica di segretezza è automaticamente declassificata a livello inferiore quando sono trascorsi cinque anni dalla data di apposizione; decorso un ulteriore periodo di cinque anni, cessa comunque ogni vincolo di classifica.

6. La declassificazione automatica non si applica quando, con provvedimento motivato, i termini di efficacia del vincolo sono prorogati dal soggetto che ha proceduto alla classifica o, nel caso di proroga oltre il termine di quindici anni, dal Presidente del Consiglio dei ministri.

7. Il Presidente del Consiglio dei ministri verifica il rispetto delle norme in materia di classifiche di segretezza. Con apposito regolamento sono determinati l'ambito dei singoli livelli di segretezza, i soggetti cui è conferito il potere di classifica e gli uffici che, nell'ambito della pubblica amministrazione, sono collegati all'esercizio delle funzioni di informazione per la sicurezza della Repubblica, nonché i criteri per l'individuazione delle materie oggetto di classifica e i modi di accesso nei luoghi militari o in quelli definiti di interesse per la sicurezza della Repubblica.

8. Qualora l'autorità giudiziaria ordini l'esibizione di documenti classificati per i quali non sia opposto il segreto di Stato, gli atti sono consegnati all'autorità giudiziaria richiedente, che ne cura la conservazione con modalità che ne tutelino la riservatezza, garantendo il diritto delle parti nel procedimento a prenderne visione senza estrarne copia.

9. Chiunque illegittimamente distrugge documenti del DIS o dei servizi di informazione per la sicurezza, in ogni stadio della declassificazione, nonché quelli privi di ogni vincolo per decorso dei termini, è punito con la reclusione da uno a cinque anni.».

Note all'art. 10:

— Per il testo dell'articolo 1, comma 2, lettera *b)* del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note all'articolo 1.

— Per il testo dell'articolo 4, comma 3, lettera *l)*, della citata legge 3 agosto 2007, n. 124, si veda nelle note all'articolo 1.

21G00089

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELLO SVILUPPO ECONOMICO

DECRETO 3 giugno 2021.

Sostituzione del commissario liquidatore della «Vignale III - società cooperativa edilizia a responsabilità limitata», in Roma.

IL DIRETTORE GENERALE
PER LA VIGILANZA SUGLI ENTI COOPERATIVI
SULLE SOCIETÀ E SUL SISTEMA CAMERALE

Visto l'art. 2545-*septiesdecies* del codice civile;

Visto l'art. 1 della legge n. 400/1975;

Visto il decreto-legge 6 luglio 2012, n. 95, convertito nella legge 7 agosto 2012, n. 135;

Visto il decreto del Ministro dello sviluppo economico in data 17 gennaio 2007, concernente la rideterminazione dell'importo minimo di bilancio per la nomina del commissario liquidatore negli scioglimenti per atto d'autorità di società cooperative, ai sensi dell'art. 2545-*septiesdecies* del codice civile;

Visto il decreto del Presidente del Consiglio dei ministri 19 giugno 2019, n. 93, recante il regolamento di organizzazione del Ministero dello sviluppo economico, per le competenze in materia di vigilanza sugli enti cooperativi;

Visto il decreto del Presidente del Consiglio dei ministri 12 dicembre 2019, n. 178, recante «Regolamento di riorganizzazione del Ministero dello sviluppo economico, ai sensi dell'art. 2, comma 16, del decreto-legge 21 settembre 2019, n. 104, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 132»;

Visto il decreto ministeriale del 4 febbraio 2005, con il quale la società cooperativa «Vignale III - società cooperativa edilizia a responsabilità limitata», con sede in Roma (RM), (codice fiscale 04540791003), è stata sciolta ai sensi dell'art. 2545-*septiesdecies* del codice civile e il dott. Marco Fantone ne è stato nominato commissario liquidatore;

Vista la richiesta di applicazione di misure cautelari personali e reali avanzata dalla Procura della Repubblica presso il Tribunale di Roma e la conseguente ordinanza n. 7287/2020 R.G. G.I.P., emessa dal Giudice per le indagini preliminari, con la quale è stata disposta nei confronti del dott. Marco Fantone la misura cautelare personale della custodia in carcere, nonché il sequestro dei beni;

Tenuto conto che nella fattispecie sussistono evidenti e motivate ragioni di pubblico interesse supportanti l'adozione di un provvedimento cautelare sia a tutela degli interessi sottesi alla stessa procedura liquidatoria, sia a tutela dell'affidamento riposto dai terzi nell'ambito dei rapporti discendenti dalla medesima procedura liquidatoria;

Preso atto che sussistono le gravi ragioni richieste dall'art. 21-*quater*, secondo comma, della legge n. 241/1990 e successive modificazioni ed integrazioni, ai fini dell'adozione del presente provvedimento cautelare e che, pertanto, per i motivi illustrati è urgente la sospensione dell'esecutività del citato decreto ministeriale del 4 febbraio 2005 nella parte riguardante la nomina del dott. Marco Fantone quale commissario liquidatore della società cooperativa «Vignale III - società cooperativa edilizia a responsabilità limitata», con sede in Roma (RM);

Considerato che, ai sensi dell'art. 7 della legge 7 agosto 1990, n. 241, con nota ministeriale n. 0147742 del 13 maggio 2021, all'interessato è stata data comunicazione dell'avvio del procedimento di sospensione in applicazione dell'art. 21-*quater*, secondo comma, della legge n. 241/1990;

Ritenuto necessario, altresì, provvedere alla sostituzione del dott. Marco Fantone dall'incarico di commissario liquidatore della società sopra indicata;

Considerato che il nominativo del professionista cui affidare l'incarico di commissario liquidatore è stato selezionato nell'ambito di un *cluster* predisposto sulla base dei requisiti professionali e di prossimità territoriale e in considerazione delle dichiarazioni di disponibilità all'assunzione dell'incarico presentate dai professionisti interessati, conformemente a quanto prescritto dalla circolare del direttore generale del 4 aprile 2018 recante «Banca dati dei professionisti interessati alla attribuzione di incarichi *ex* articoli 2545-*terdecies*, 2545-*sexiesdecies*, 2545-*septiesdecies*, secondo comma e 2545-*octiesdecies* del codice civile», pubblicata sul sito internet del Ministero;