SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

N. 240

ATTO DEL GOVERNO
SOTTOPOSTO A PARERE PARLAMENTARE

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

*(Parere ai sensi dell'articolo 1, commi 3 e 4-*bis*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)*

(Trasmesso alla Presidenza del Senato il 14 gennaio 2021)

Il Ministro
per i rapporti con il Parlamento
DRP/II/XVIII/D119/21

Roma, 14 gennaio 2021

trasmetto, al fine dell'espressione del parere da parte delle Commissioni parlamentari competenti per materia, lo schema di decreto del Presidente del Consiglio dei ministri recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione all'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Federico D'Incà

Sen. Maria Elisabetta ALBERTI CASELLATI
Presidente del Senato della Repubblica
ROMA

MODULARIO
P.C.M. 73

MOD. 111

Roma, 13 GEN. 2021

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

N. DAGL 4.3.2.1/2020/120

Presidenza del Consiglio dei Ministri
DAGL 0000399 P-
del 13/01/2021

31429139

AL DIPARTIMENTO PER I RAPPORTI CON IL PARLAMENTO
Alla cortese attenzione del Capo Dipartimento

OGGETTO: Schema di decreto del Presidente del Consiglio dei ministri recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Si trasmette lo schema di decreto del Presidente del Consiglio dei ministri indicato in oggetto ai fini della trasmissione alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle Commissioni parlamentari competenti per materia, ai sensi dell'articolo 1, comma 4-*bis* del decreto-legge 21 settembre 2019 n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

IL CAPO DIPARTIMENTO
Presidente Ermanno de Francisco

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 regolamento adottato con decreto del Presidente della Repubblica ..... n. ....., ai sensi dell'articolo 1, comma 6, del decreto-legge n. 105 del 2019, recante.....;

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 .....;

ACQUISITI i pareri della Commissione ..... della Camera dei deputati in data ..... e della Commissione ..... del Senato della Repubblica in data.....;

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.

CAPO II
NOTIFICHE DI INCIDENTE

Art. 2
(*Tassonomia degli incidenti*)

1. Nelle tabelle n. 1 e n. 2 in allegato A al presente regolamento sono classificati gli incidenti aventi impatto sui beni ICT. Le due tabelle sono distinte a seconda della gravità degli incidenti, recando i meno gravi nella prima e i più gravi nella seconda, anche tenuto conto della tempistica necessaria per una risposta efficace.

Art. 3

(Notifica degli incidenti aventi impatto su beni ICT)

1. 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 comma 3.

2. I soggetti inclusi nel perimetro procedono alla notifica di cui al comma 1 anche nei casi in cui uno degli incidenti individuati nelle tabelle di cui all'allegato A abbia comunque impatto su un bene ICT di rispettiva pertinenza, ancorché si verifichi a carico di un sistema informativo, ovvero un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'articolo 7, comma 2, del regolamento adottato con il decreto del Presidente del Consiglio dei ministri di cui all'articolo 1, comma 2, del decreto-legge, condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero *software* di base quali sistemi operativi e di virtualizzazione.

3. La notifica avviene, 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:

a) entro il termine di sei ore dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 1 di cui all'allegato A;

b) entro il termine di un'ora dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 2 di cui all'allegato A.

4. 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.

5. 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 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.

6. Su richiesta del CSIRT italiano, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1 e 2 provvede, tramite i canali di comunicazione di cui al comma 3 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.

7. 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 e 2, tramite i canali di comunicazione di cui al comma 3, 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.

8. 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.

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.

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.

Art. 5
(*Trasmissione delle notifiche*)

1. Il DIS inoltra le notifiche ricevute ai sensi dell'articolo 3, nonché dell'articolo 4 nel caso in cui tali notifiche volontarie vengano trattate:

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 stesse 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 stesse provengano da un soggetto privato.

2. 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.

3. Le modalità per gli inoltri delle notifiche previsti 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.

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 e ne comunicano l'avvenuta adozione e 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, con il modello reso disponibile dal DIS 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, 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 avvenga in una data antecedente a quella di entrata in vigore del presente

regolamento, entro sei mesi da quest'ultima data. Nell'ipotesi in cui le abbiano già adottate, comunicano, altresì, le modalità di adozione delle misure di sicurezza di cui alla categoria B dell'appendice n. 2 dell'allegato B;

b) per quelle appartenenti alla categoria B di cui all'appendice n. 2 dell'allegato B, entro ventiquattro 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 avvenga in una data antecedente a quella di entrata in vigore del presente regolamento, entro ventiquattro mesi da quest'ultima data.

2. Qualora un soggetto incluso nel perimetro proceda, ai sensi degli articoli 7 e 9 del regolamento adottato con 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 ventiquattro mesi dall'aggiornamento dell'elenco dei beni ICT.

3. 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.

4. 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 alle categorie 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 60 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,

Allegato A

(articolo 2)

Tassonomia degli incidenti

TABELLA 1

Identificativo	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		Dati non intenzionalmente accessibili a soggetti non autorizzati.
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		Impossibilità prolungata di accesso fisico alle componenti
ICP-A-11	**Installazione (*Establish persistence*)**	**Ottenimento di privilegi di livello superiore (*Privilege Escalation*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore.
ICP-A-12		**Persistenza (*Persistence*)**. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere persistenza di codice malevolo o d'accesso.

Identificativo	Categoria	Descrizione
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. le vulnerabilità di cui alla sottocategoria ID.RA-1 e, qualora disponibili, 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 o relativi al loro funzionamento, alla loro descrizione o alla loro sicurezza, anche parziale, 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 ricompresi i siti di *backup* e di *disaster recovery,* nonché le infrastrutture deputate alle funzioni di sicurezza che hanno accesso ai predetti dati.
2. Le disposizioni di cui al punto 1 non si applicano alle sedi diplomatiche o consolari.
3. Esiste un documento aggiornato che descrive in quali sedi sono conservati, trattati ovvero estratti i dati digitali relativi ai beni ICT, ovvero le fattispecie di cui al punto 2.
4. 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

Misure	Categoria
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.

RELAZIONE ILLUSTRATIVA

Schema di decreto del Presidente del Consiglio dei ministri, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

In ragione della rapida evoluzione tecnologica, il rischio che dalle minacce alle reti, ai sistemi informativi e ai servizi informatici, necessari per l'espletamento di funzioni essenziali dello Stato o per la prestazione di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, possa derivare un pregiudizio per la sicurezza nazionale, ha reso necessario e urgente garantire un livello elevato di sicurezza di tali reti, sistemi informativi e servizi informatici.

Pertanto, con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (di seguito indicato "decreto-legge"), è stato istituito il perimetro di sicurezza nazionale cibernetica ed è stato rafforzato il quadro normativo in tema di esercizio dei poteri speciali nei settori di rilevanza strategica.

Il presente schema di provvedimento interviene nel quadro normativo sin qui delineatosi con il decreto-legge e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè 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, di recente pubblicazione nella *Gazzetta Ufficiale* n. 261, del 21 ottobre 2020.

Nello specifico, il presente schema di decreto è volto a dare attuazione alle disposizioni di cui all'articolo 1, comma 3, del decreto-legge. Tali disposizioni prevedono che, entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, con decreto del Presidente del Consiglio dei ministri – adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) – che disciplini, altresì, i relativi termini e le modalità attuative:

a) siano definite le procedure secondo cui i soggetti individuati ai sensi dell'articolo 1, comma 2, lettera *a)*, del decreto-legge, inclusi nell'elenco di cui al comma 2-*bis* del medesimo articolo, notificano al CSIRT italiano gli incidenti aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge. È quindi previsto che il CSIRT italiano inoltri tempestivamente tali notifiche al Dipartimento delle informazioni per la sicurezza (DIS), anche per le attività demandate al Nucleo

per la sicurezza cibernetica, e che il DIS assicuri 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, nell'ipotesi in cui tali notifiche provengano 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, nell'ipotesi in cui le notifiche provengano da un soggetto privato;

b) siano stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, tenendo conto degli *standard* definiti a livello internazionale e dell'Unione europea. Il decreto-legge definisce, quindi, nove ambiti ai quali le misure stabilite dovranno attenere. Nello specifico, l'articolo 1, comma 3, lettera *b)*, prevede che le misure siano 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.

Con riferimento all'elaborazione di tali misure, l'articolo 1, comma 4, del decreto-legge, prevede che vi provvedano, secondo gli ambiti di competenza delineati dallo stesso decreto-legge, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il DIS.

Al fine di assicurare il coordinamento tra il quadro normativo introdotto con l'istituzione del perimetro di sicurezza nazionale cibernetica e le disposizioni già previste, in materia di adozione di misure di sicurezza e obblighi di notifica degli incidenti, da altri plessi dispositivi vigenti (nello specifico, la disciplina di cui al decreto legislativo 18 maggio 2018, n. 65, il c.d. decreto legislativo NIS, nonché quella di cui al decreto legislativo 1° agosto 2003, n. 259, il codice delle comunicazioni elettroniche, e alle correlate disposizioni attuative), l'articolo 1,

comma 8, del decreto-legge, dispone che i soggetti rispettivamente tenuti al rispetto di tali disposizioni:

a) osservino le misure di sicurezza previste dal decreto legislativo NIS, ovvero dal codice delle comunicazioni elettroniche, ove queste siano di livello almeno equivalente a quelle adottate ai sensi dell'articolo 1, comma 3, lettera *b)*, del decreto-legge, e che eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal decreto-legge siano definite – a seconda degli ambiti di rispettiva competenza – dalla Presidenza del Consiglio dei ministri, ovvero dal Ministero dello sviluppo economico avvalendosi anche del Centro di valutazione e certificazione nazionale (CVCN); è quindi previsto che, ove necessario, la Presidenza del Consiglio di ministri e il Ministero dello sviluppo economico si raccordino con le autorità competenti di cui all'art. 7 del decreto legislativo NIS;

b) assolvano l'obbligo di notifica di cui all'articolo 1, comma 3, lettera *a)*, del decreto-legge, disponendo che ciò costituisca anche adempimento degli obblighi rispettivamente previsti dal decreto legislativo NIS, ovvero ai sensi del codice delle comunicazioni elettroniche e delle correlate disposizioni attuative. A tal fine, prevede che, oltre a quanto previsto dall'articolo 1, comma 3, lettera *a)*, del decreto-legge, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice delle comunicazioni elettroniche, il CSIRT italiano provveda a inoltrare le notifiche ricevute all'autorità competente di cui all'articolo 7 del decreto legislativo NIS.

È, poi, previsto dall'articolo 1, comma 6, lettera *c)*, del decreto-legge, che le attività di ispezione e verifica, in relazione anche a quanto disposto in materia di notifiche di incidenti e misure di sicurezza, siano svolte dalla Presidenza del Consiglio dei ministri e dal Ministero dello sviluppo economico, per i rispettivi ambiti di competenza definiti dal decreto-legge. È quindi disposto che per le reti, i sistemi informativi e i servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge – che siano 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 siano svolte dalle strutture specializzate 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.

Con riguardo alle procedure di adozione e aggiornamento del provvedimento di attuazione dell'articolo 1, comma 3, del decreto-legge, il comma 4-*bis*, del medesimo articolo 1, dispone che lo schema di decreto venga trasmesso alla Camera dei deputati e al Senato della Repubblica, per l'espressione del parere delle Commissioni parlamentari competenti per materia, nonché al Comitato parlamentare per la sicurezza della Repubblica, mentre il successivo comma 5 dispone che all'aggiornamento si proceda secondo le medesime modalità seguite per l'adozione. All'articolo 1, comma 19-*ter*, poi, il decreto-legge dispone che, nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal

medesimo articolo 1 sia acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti siano sospesi per un periodo di quarantacinque giorni.

Sul punto la relazione tecnica allegata al decreto-legge, positivamente verificata dalla Ragioneria generale dello Stato, chiarisce che per quanto riguarda i soggetti pubblici inclusi nel perimetro, agli oneri derivanti dall'obbligo di attuare le misure di sicurezza si provvederà, a decorrere dagli esercizi finanziari 2020 e 2021, con le risorse finanziarie, umane e strumentali già previste a legislazione vigente.

Al fine di dare attuazione alle previsioni di cui all'articolo 1, commi 3 e 4, del decreto-legge, sono stati adottati appositi moduli organizzativi per la definizione delle procedure di notifica degli incidenti e per l'elaborazione e la condivisione delle misure di sicurezza, anche mediante la costituzione di appositi gruppi di lavoro, che hanno visto la partecipazione dei rappresentanti delle diverse amministrazioni interessate. A conclusione dei lavori, la condivisione tra le amministrazioni sulle diverse soluzioni tecnico-giuridiche elaborate e, quindi, sullo schema di decreto è stata, poi, assicurata nell'ambito dell'organismo tecnico di supporto al CISR di cui all'articolo 4, comma 5, del regolamento adottato con DPCM 3 aprile 2020, n. 2 (il c.d. "CISR tecnico"), integrato da un rappresentante della struttura della Presidenza del Consiglio competente per la innovazione tecnologica e la digitalizzazione, designato in ragione degli specifici compiti attribuiti alla Presidenza del Consiglio dal decreto-legge, nonché da rappresentanti del Ministero delle infrastrutture e dei trasporti, del Ministero del lavoro e delle politiche sociali, del Ministero dell'università e ricerca, nonché dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri.

Poiché la proposta di decreto ha evidenziato indici che hanno indotto a ritenerne il carattere normativo, si è ritenuto di dover richiedere il parere del Consiglio di Stato, così come avvenuto per il provvedimento di attuazione previsto dall'articolo 1, comma 2, del decreto-legge, in relazione al quale il Supremo Organo consultivo ha convenuto, in sede di parere, sulla sostanza normativa delle disposizioni ivi recate. Al riguardo, è stato considerato, infatti, che il presente decreto del Presidente del Consiglio dei ministri di attuazione delle previsioni di cui all'articolo 1, comma 3, del decreto-legge, appare rivolto a innovare l'ordinamento giuridico, introducendo disposizioni – volte a integrare il precetto delle disposizioni di rango primario – che dettano termini e procedure in materia di obblighi di notifica degli incidenti, nonché l'individuazione delle misure di sicurezza, in relazione ai sopracitati ambiti definiti dal decreto-legge, e i relativi termini e modalità di adozione da parte dei soggetti inclusi nel perimetro. Con particolare riferimento alle misure di sicurezza, il presente decreto provvede a definire il contenuto prescrittivo in relazione agli ambiti delineati dal legislatore, stabilendo quali siano le specifiche misure che i soggetti tenuti alla loro osservanza dovranno adottare, quali siano le modalità di attuazione delle disposizioni introdotte e quali i termini entro cui provvedere.

Sullo schema di decreto del Presidente del Consiglio dei ministri è, quindi, intervenuto il CISR – organo al quale spetta, in ossequio alla richiamata procedura,

la proposta di adozione – che, ai fini della trasmissione al Consiglio di Stato, ha favorevolmente deliberato sul testo, in via preliminare, nella seduta del 27 ottobre 2020.

Tanto premesso, si illustra di seguito il contenuto del decreto e delle singole disposizioni con le quali si dà attuazione alle prescrizioni indicate dal decreto-legge.

Il presente decreto si compone di 11 articoli suddivisi in IV capi, di cui il capo I dedicato alle disposizioni generali, il capo II alle notifiche di incidente, il capo III alle misure di sicurezza e il capo IV alle disposizioni finali, ed è integrato, in ragione della complessità e del livello tecnico della disciplina, da 3 allegati, di cui il primo (allegato A), previsto dall'articolo 2, recante due tabelle di classificazione degli incidenti aventi impatto sui beni ICT (nel significato che verrà di seguito specificato in sede di illustrazione dell'articolo 1), il secondo (allegato B), previsto dall'articolo 7, recante le misure di sicurezza, e il terzo (allegato C), previsto dall'articolo 9, recante misure minime per la tutela delle informazioni.

L'**articolo 1**, del capo I, è dedicato alle definizioni. Nello specifico, nell'ottica di garantire la coerenza con l'assetto definitorio delineato dagli altri provvedimenti di attuazione del decreto-legge (il richiamato regolamento adottato in attuazione dell'articolo 1, comma 2, del decreto-legge, con DPCM n. 131 del 2020, e lo schema di regolamento da adottare con DPR, in attuazione del comma 6 del medesimo articolo 1 del decreto-legge, sul quale è stato reso il parere del Consiglio di Stato - Sezione consultiva per gli atti normativi, nell'adunanza del 20 ottobre u.s.), l'articolo 1 reca soltanto quelle definizioni ritenute necessarie a chiarire la portata delle disposizioni contenute nello schema decreto, soffermandosi, in particolare, su quei termini, o locuzioni, ai quali sono stati attribuiti, ai fini del presente decreto, significati tecnici specifici. Si evidenziano, in particolare, le definizioni di:

- "*soggetti inclusi nel perimetro*", con cui si intende fare riferimento ai soggetti che siano stati individuati secondo le procedure di cui all'articolo 1, comma 2, lettera *a)*, del decreto-legge, e inclusi nell'elencazione contenuta nell'atto amministrativo adottato ai sensi dell'articolo 1, comma 2-*bis*, del decreto-legge;
- "*bene ICT*", conforme alla definizione, già recata dal DPCM n. 131 del 2020, che è stata adeguata al fine di tenere conto, in ragione dell'avanzamento del processo di attuazione del perimetro di sicurezza nazionale cibernetica, dell'inserimento, da parte di ciascuno dei soggetti inclusi nel perimetro, dei beni ICT nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge, che costituisce un antecedente logico rispetto all'ambito normativo di cui al presente decreto;
- "*impatto sul bene ICT*", con cui, infine, si è provveduto a specificare, avuto riguardo a un bene ICT, cosa debba intendersi per "*impatto*", atteso che la nozione comune di "*impatto*" fa riferimento ai concetti di "*urto*", che poco sembra attagliarsi alla realtà cibernetica, o di "*evento*", di portata semantica

molto ampia. È stato così individuato e specificato, in assenza di disposizioni definitorie nel provvedimento legislativo d'urgenza, l'ambito di operatività della disposizione di cui all'articolo 1, comma 3, lettera *a)*, del decreto-legge, che impone l'obbligo di notifica al CSIRT italiano per "*gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera* b)". La formulazione della definizione ha trovato ancoraggio al concetto di "*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*", già formulato nell'ambito dell'articolo 7, comma 2, lettera *a)*, numero 1), del richiamato regolamento adottato con DPCM n. 131 del 2020.

Al fine di giungere, pertanto, a delineare il significato, in sede di normativa di attuazione, del concetto di "*incidenti aventi impatto su beni ICT*" recato dalla disposizione di rango primario, infine, si è ritenuto di non doversi discostare dalla definizione di "*incidente*", già adottata nell'ambito del quadro attuativo delle disposizioni del decreto-legge, come sin qui delineatosi con i provvedimenti previsti dall'articolo 1, commi 2 e 6, che è stata, pertanto, riproposta.

L'**articolo 2** apre il capo II dedicato alle notifiche di incidente. Nello specifico, avuto anche riguardo alle prassi e agli *standard* definiti a livello internazionale e dell'Unione europea, sono stati classificati, in due tabelle riportate in allegato A al presente decreto, quegli incidenti per i quali il decreto-legge pone l'obbligo di notifica in capo ai soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge (nelle definizioni di cui all'articolo 1 indicati quali "*soggetti inclusi nel perimetro*"), e cioè gli incidenti aventi impatto sui beni ICT. In ossequio alla definizione di incidente recata dal regolamento adottato con DPCM n. 131 del 2020, la tassonomia degli incidenti risponde all'esigenza di strutturare un approccio che ne ricomprenda una casistica ampia, indipendentemente dall'intenzionalità o dall'accidentalità che li possa caratterizzare. Pertanto, si è provveduto a unificare due modelli largamente impiegati dalle comunità internazionali, scientifica e di sicurezza informatica, traendo spunto, al contempo, da standard *de facto* e da migliori pratiche anche internazionali. La suddivisione nelle due tabelle è stata operata a seconda della gravità degli incidenti, recando i meno gravi nella prima e i più gravi nella seconda, anche tenuto conto della tempistica necessaria per una risposta efficace. Per quanto concerne la tabella n. 1, vi si trovano elencate, in particolare, le tipologie di incidenti che si possono configurare come precursori rispetto a ulteriori incidenti idonei, a loro volta, a determinare un impatto ancora più significativo sui beni ICT. Tale ultima tipologia di incidenti è stata inclusa nella tabella n. 2. A tale suddivisione corrisponde, come verrà di seguito meglio illustrato nell'ambito dell'articolo 3, una diversa definizione dei termini per l'adempimento dell'obbligo di notifica: sei ore per quelli della tabella n. 1 e un'ora per quelli della tabella n. 2. La scelta di indicare un termine più breve e stringente (un'ora) per gli incidenti di cui alla tabella n. 2 è legata alla necessità di assicurare tempi più rapidi di reazione da parte dell'intera architettura nazionale *cyber* per gli incidenti più gravi, anche in ragione della portata degli impatti discendenti.

L'**articolo 3** delinea le procedure e definisce i termini per la notifica al CSIRT italiano – istituito presso il DIS ai sensi dell'articolo 8, comma 1, del decreto legislativo 18 maggio 2018, n. 65 (c.d. decreto legislativo NIS) – degli incidenti aventi impatto su un bene ICT, e cioè di uno degli incidenti classificati nelle tabelle in allegato A al presente decreto. La disposizione chiarisce, altresì, che deve essere notificato uno degli incidenti di cui all'allegato A, che, in aderenza al dettato legislativo, abbia comunque impatto su un bene ICT, anche nell'ipotesi in cui l'incidente si verifichi a carico di un sistema informativo, o di un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'articolo 7, comma 2, del regolamento adottato con 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.

Per l'effettuazione della notifica, vengono individuati i canali di comunicazione del CSIRT italiano, prescrivendo, per ragioni di coerenza ordinamentale, che gli stessi abbiano i requisiti di cui al punto 1, lettera *a)*, dell'allegato I, del decreto legislativo NIS, secondo modalità definite dal CSIRT italiano e rese disponibili sul sito Internet di tale organo.

Vengono, quindi, indicati i termini entro i quali adempiere all'obbligo di notifica: entro sei ore per gli incidenti classificati in tabella n. 1 ed entro un'ora per gli incidenti classificati in tabella n. 2. La definizione dei termini di notifica, di cui il più breve fissato in un'ora, è stata determinata a valle di una ricognizione dei termini di notifica esistenti in altri settori, come, in particolare, quello della sicurezza delle reti e dei sistemi informativi di cui al decreto legislativo NIS, ovvero quello della protezione dei dati personali di cui al Regolamento generale sulla protezione dei dati personali dell'UE (il "GDPR"), nonché quello relativo ai servizi di pagamento nel mercato interno disciplinato dalla direttiva (UE) 2015/2366. Sono stati tenuti in considerazione, quindi, lo specifico ambito in cui operano le disposizioni del decreto-legge, e cioè quello della sicurezza nazionale cibernetica, e l'essenzialità del fattore temporale ai fini di un rapido intervento in caso di incidente.

Per ciò che riguarda il momento iniziale dal quale decorre il termine per l'adempimento dell'obbligo di notifica, esso è stato individuato nel momento in cui il soggetto incluso nel perimetro, titolare del bene ICT impattato dall'incidente, "*ne è venuto a conoscenza*". Tale soluzione, la cui formulazione è stata mutuata dalla disciplina in materia di protezione dei dati personali e di notifica dei c.d. *data breach*, è volta, da un lato, a dare atto della peculiarità degli incidenti informatici, la cui scoperta può avvenire, successivamente, anche a distanza di molto tempo; dall'altro, a consentire ai soggetti titolari dei beni ICT di poter effettuare la notifica nei termini previsti all'esito di un processo di "*triage*", finalizzato alla verifica preliminare in ordine alla circostanza che l'incidente verificatosi presenti gli elementi essenziali contenuti nelle fattispecie di incidente classificate in allegato A.

Successivamente al momento iniziale della notifica, anche in considerazione dei brevi termini fissati, è previsto che il soggetto debba provvedere a una tempestiva

integrazione della notifica stessa, qualora venga a conoscenza di nuovi elementi significativi di natura tecnica o comunque correlati all'incidente oggetto di notifica (comma 4). È, infine, prevista la possibilità per il CSIRT italiano di richiedere al soggetto notificante sia elementi di aggiornamento sull'incidente in corso (comma 6), sia, nella fase di risoluzione dell'incidente (individuata nel momento in cui siano stati definiti ed avviati da parte del soggetto notificante i piani di attuazione delle attività per il ripristino dei beni ICT impattati dall'incidente), la trasmissione di una relazione tecnica che dia conto degli elementi significativi dell'incidente e, in particolare, delle conseguenze dell'impatto sui beni ICT e delle azioni intraprese per porvi rimedio (comma 7).

Al fine di coordinare gli obblighi del soggetto incluso nel perimetro relativi alle notifiche di incidente, previsti dal decreto-legge, con le eventuali esigenze di segretezza investigativa, discendenti dall'avvio di indagini da parte dell'autorità giudiziaria, viene previsto che il soggetto notificante proceda all'integrazione della notifica (comma 4), fornisca su richiesta del CSIRT italiano elementi di aggiornamento (comma 6), e trasmetta la relazione tecnica che illustra gli elementi significativi dell'incidente al CSIRT italiano (comma 7), salvo che l'autorità giudiziaria procedente non abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

Con riferimento, infine, al comma 5, allo scopo di dare attuazione alle disposizioni di cui all'articolo 1, comma 8, lettera *b)*, del decreto-legge, sono previsti gli opportuni raccordi per l'assolvimento degli obblighi di notifica previsti dalla disciplina di cui al decreto legislativo NIS e al codice delle comunicazioni elettroniche (e correlate disposizioni attuative). In particolare, è stabilito che la notifica di incidente effettuata nell'ambito della disciplina introdotta dal decreto-legge valga anche ai fini dell'adempimento dell'obbligo di notifica previsto dal codice delle comunicazioni elettroniche e dal decreto legislativo NIS. In tale ipotesi, i soggetti interessati, qualora l'incidente rilevi anche ai fini del decreto legislativo NIS, ovvero del codice delle comunicazioni elettroniche, nell'effettuare la notifica al CSIRT italiano, indicano, rispettivamente, l'autorità competente NIS (alla quale il CSIRT italiano provvederà ad inoltrare la notifica), ovvero che la medesima notifica costituisce anche adempimento dell'obbligo previsto dalla disciplina di cui al codice delle comunicazioni elettroniche e correlate disposizioni attuative. In via ricognitiva, poi, viene precisato che restano fermi gli obblighi di notifica, secondo le relative procedure, previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche e relative disposizioni attuative per quegli incidenti che non rientrano nell'ambito di applicazione del decreto-legge.

L'**articolo 4** è volto a disciplinare la possibilità per i soggetti inclusi nel perimetro di notificare incidenti non rientranti tra le categorie per le quali è prevista la notifica obbligatoria. Con tale disposizione in materia di notifiche volontarie, che in parte recepisce analogo istituto previsto nell'ambito del decreto legislativo NIS, si intende poter consentire, da un lato, ai soggetti, di comunicare incidenti che ritengano comunque significativi e meritevoli di essere portati all'attenzione del

CSIRT italiano, dall'altro, allo stesso CSIRT italiano, di ampliare il quadro conoscitivo e statistico relativo alle tipologie di incidenti che occorrono a danno delle reti, dei sistemi informativi e dei servizi informatici dei soggetti inclusi nel perimetro. Ciò, anche in aderenza ai compiti assegnati al CSIRT italiano dal decreto legislativo NIS (articolo 8 e allegato I, punto 2), tra i quali rientrano il monitoraggio degli incidenti a livello nazionale e l'analisi dinamica dei rischi e degli incidenti.

L'**articolo 5** è dedicato, in ossequio alle previsioni di cui all'articolo 1, commi 3, lettera *a)*, e 8, lettera *b)*, del decreto-legge, alla trasmissione delle notifiche ricevute dal CSIRT italiano ai diversi soggetti istituzionali destinati a riceverle. È inoltre prevista la possibilità di stipulare apposite intese con ciascuna delle amministrazioni interessate, al fine di concordare le modalità di trasmissione delle notifiche. Tenuto conto che, per le attività di ispezione e verifica relative, in particolare, ai beni ICT connessi alla difesa e sicurezza militare dello Stato, sono competenti, ai sensi dell'articolo 1, comma 6, lettera *c)*, terzo periodo, del decreto-legge, le strutture specializzate del Ministero della difesa, la possibilità di stipulare apposite intese è stata estesa anche in relazione a quell'amministrazione in merito alle notifiche di incidente che la stessa provvede a effettuare.

L'**articolo 6** reca disposizioni di carattere ricognitivo. In ragione dell'esclusione dall'elenco dei beni ICT per le reti, per i sistemi informativi e per i servizi informatici attinenti alla gestione delle informazioni classificate, disposta dall'articolo 1, comma 2, lettera *b*), del decreto-legge, viene confermato, per ragioni di chiarezza ordinamentale, che i relativi incidenti non soggiacciano all'obbligo di notifica di cui al presente decreto. È confermato, quindi, che per tali incidenti 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.

L'**articolo 7** apre il capo III dedicato alle misure volte a garantire elevati livelli di sicurezza dei beni ICT. Le misure di carattere tecnico e organizzativo stabilite con il presente decreto, riportate sistematicamente nell'allegato B, integrano di contenuto normativo i richiamati ambiti delineati dal legislatore primario nelle disposizioni di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge (tra questi, a titolo esemplificativo, si evidenziano quelli relativi "*alla struttura organizzativa preposta alla gestione della sicurezza*", "*alle politiche di sicurezza e alla gestione del rischio*", "*alla sicurezza fisica e logica e dei dati*").

Per l'individuazione delle misure, è stato assunto, quale base di riferimento, 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 Laboratorio nazionale di Cybersecurity 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). Tale

strumento scientifico ampiamente riconosciuto a livello nazionale è stato, quindi, adeguato allo specifico contesto operativo delineato dal perimetro di sicurezza nazionale cibernetica. A tale riguardo, giova evidenziare che il *Framework* nazionale, da un lato, ha rappresentato, sin dal 2015, uno strumento elaborato in condivisione tra realtà istituzionali e soggetti privati, pubblicamente disponibile con la finalità di promuovere un approccio volontario e omogeneo per affrontare la cybersicurezza, al fine di ridurre il rischio legato alla minaccia nell'ambito cyber; dall'altro, è stato assunto, anche nell'ambito della disciplina di recepimento della direttiva NIS, quale base di riferimento da parte delle autorità competenti NIS per l'adozione delle linee guida sulle misure di sicurezza di cui gli operatori di servizi essenziali (OSE) devono tener conto ai sensi di quella normativa. Il *Framework* nazionale, peraltro, fa a sua volta riferimento ad altri autorevoli strumenti internazionali in materia, quali, in particolare, il *Framework for Improving Critical Infrastructure Cybersecurity* del National Institute of Standards and Technology (NIST).

La scelta di adottare, quale base di riferimento, il *Framework* nazionale ha anche consentito di realizzare un opportuno punto di equilibrio tra il livello prescrittivo, come definito dal legislatore regolamentare, e quello della concreta applicazione delle diverse misure, che viene demandato a ciascun soggetto nell'ambito della rispettiva realtà organizzativa. In tal senso, infatti, il presente decreto, con le misure di sicurezza che ha provveduto a individuare, intende prescrivere ai soggetti obblighi di natura tecnica e organizzativa e fornire, per ciascuna di esse, una specifica più dettagliata dell'implementazione minima attesa, nonché delle modalità richieste al fine di descriverne l'adozione e dimostrarne l'attuazione. Allo stesso tempo, la scelta sulle modalità di attuazione delle misure viene necessariamente rimessa alle valutazioni di ciascun soggetto incluso nel perimetro – in relazione alle proprie specifiche caratteristiche tecniche e organizzative – che avverranno anche a seguito delle analisi del rischio che condurrà ciascun soggetto incluso nel perimetro, tra cui quella già prevista, ai fini dell'individuazione dei beni ICT, dal regolamento adottato con DPCM n. 131 del 2020.

Le misure sono state organizzate sistematicamente nell'allegato B 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. Ciò al fine di consentire un più immediato riferimento e ausilio alla lettura e all'applicazione delle misure in parola.

Le misure di cui all'allegato B sono caratterizzate dalla misurabilità. Nello specifico, anche al fine di poter agevolare lo svolgimento delle attività di verifica e ispettive, ogni sottocategoria dà luogo alla produzione di un'evidenza documentale o fisica, immediatamente apprezzabile e valutabile. A titolo esemplificativo, si considerino: il "*documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity*" di cui alla sottocategoria 2.2.2 (ID.GV-4), il "*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" di cui alla sottocategoria 2.3.1 (ID.RA-1), ovvero ancora la "*pianificazione aggiornata degli audit di sicurezza previsti*" e il "*registro degli audit di sicurezza effettuati con la relativa documentazione*" previsti nell'ambito della sottocategoria 3.1.1. (PR.AC-1).

Le misure di sicurezza individuate dal presente decreto corrispondono ai nove ambiti delineati dal decreto-legge all'articolo 1, comma 3, lettera *b)*. In ragione della richiamata scelta operata nei sensi di assumere, quale base di riferimento, il *Framework* nazionale, e delle conseguenti ricadute redazionali e sistematiche sull'elaborazione del testo regolamentare comprensivo degli allegati, l'allegato B è corredato (in appendice n. 1) di una tabella di corrispondenza tra gli ambiti del decreto-legge e le misure individuate per ciascuno di tali ambiti. Nel caso in cui una misura attenga a più ambiti, la stessa è stata riportata in corrispondenza di ciascuno di essi. Nel caso in cui, infine, in relazione ad uno specifico ambito trovi applicazione soltanto una parte specifica di una determinata misura, anche tale limitazione è stata opportunamente evidenziata.

Al fine del completamento del quadro di protezione dei "beni ICT" infine, sono indicate, ai punti 2.1.2 (ID.AM-2) e 2.5.2 (ID.SC-2) del richiamato allegato B, previsioni di contenuto esortativo, chiaramente introdotte con la formula "*si raccomanda*", le cui determinazioni in merito a una loro attuazione sono demandate a ciascun soggetto incluso nel perimetro.

L'**articolo 8** è dedicato alla definizione delle modalità con le quali i soggetti inclusi nel perimetro debbano adottare, per ciascun bene ICT di rispettiva pertinenza, le misure di cui all'allegato B, nonché dei relativi termini entro i quali provvedere. In particolare, sono previsti due differenti termini di adozione delle misure, sei mesi e ventiquattro mesi, distinti a seconda che si tratti di misure, rispettivamente, di più immediata attuazione, ovvero per la cui implementazione siano necessari interventi che richiedano, potenzialmente, una più impegnativa attività sotto i profili progettuali e programmatici. In ragione di tale distinzione, le misure individuate nell'allegato B sono state suddivise in due macro-categorie, categoria A (da adottare entro 6 mesi) e categoria B (da adottare entro 24 mesi), e di tale classificazione, per pronto e chiaro riferimento dei soggetti tenuti all'adozione delle misure nei diversi tempi previsti, è stato dato atto in un'apposita tabella (in appendice n. 2 all'allegato B).

Per l'individuazione del momento iniziale dal quale far decorrere il termine entro il quale adottare le misure di sicurezza, si è dovuto necessariamente tenere conto del quadro dispositivo delineato dall'articolo 1, comma 2, del decreto-legge e dal regolamento adottato con DPCM n. 131 del 2020 adottato in sua attuazione. In capo ai soggetti inclusi nel perimetro, infatti, è previsto l'obbligo, in particolare, di predisporre l'elenco dei beni ICT di rispettiva pertinenza e di trasmettere tale elenco entro sei mesi dalla data in cui è avvenuta la comunicazione di inclusione nel perimetro di sicurezza nazionale cibernetica. La predisposizione dell'elenco dei

beni ICT che, come già sopra anticipato, avviene, da parte di ciascun soggetto incluso nel perimetro, in esito all'effettuazione di un'analisi del rischio per ogni funzione essenziale dello Stato esercitata o servizio essenziale prestato, rappresenta, pertanto, un presupposto logico e di fatto per l'adozione delle misure di sicurezza per ciascuno dei beni ICT individuati nel predetto elenco. Conseguentemente, è stato stabilito che le misure di categoria A e B debbano essere adottate, rispettivamente, entro sei e ventiquattro mesi, dalla data di trasmissione (mediante la piattaforma digitale costituita presso il DIS ai sensi dell'articolo 9 del DPCM n. 131/2020) degli elenchi dei beni ICT. Infine, non essendo possibile conoscere a priori le tempistiche di adozione, ai sensi dell'articolo 1, comma 2-*bis*, del decreto-legge, dell'atto amministrativo recante l'elencazione dei soggetti inclusi nel perimetro, né la data in cui ciascuno di tali soggetti provvederà a trasmettere l'elenco dei beni ICT di rispettiva pertinenza, è stato previsto che, qualora la trasmissione dell'elenco dei beni ICT avvenga in una data antecedente a quella dell'entrata in vigore del presente decreto, i termini decorreranno da tale ultima data.

È quindi previsto che i soggetti tenuti comunichino, mediante la predetta piattaforma digitale costituita presso il DIS, le modalità con le quali hanno provveduto ad adottare le misure di sicurezza. A tal fine, è previsto l'utilizzo di un apposito modulo che verrà reso disponibile dal DIS.

Ai fini dello svolgimento delle attività di ispezione e verifica da parte dei soggetti individuati ai sensi dell'articolo 1, comma 6, lettera *c)*, primo periodo, del decreto-legge (Presidenza del Consiglio dei ministri e Ministero dello sviluppo economico), è previsto che il DIS renda loro tempestivamente disponibili le comunicazioni ricevute da parte dei soggetti inclusi nel perimetro, relative alle modalità di adozione e agli eventuali aggiornamenti delle misure di sicurezza. Infine, poiché il decreto-legge prevede che le attività di ispezione e verifica per i beni ICT 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, siano svolte dalle competenti strutture delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, è escluso che le comunicazioni sulle misure di sicurezza concernenti tali beni ICT vengano, successivamente alla loro trasmissione e conservazione sulla piattaforma digitale costituita presso il DIS, rese disponibili alle strutture della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico.

L'**articolo 9** individua, nell'allegato C al presente decreto, misure minime di sicurezza di natura tecnica e organizzativa volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT, agli elementi delle notifiche di incidente, al modello di cui all'articolo 8 recante le modalità di adozione delle misure di sicurezza e, infine, alla documentazione relativa alle misure di sicurezza adottate da parte dei soggetti inclusi nel perimetro ai sensi degli articoli 7 e 8. Ciò, anche al fine di corrispondere all'esigenza di tutela delle informazioni emersa in sede di adozione del regolamento di cui al DPCM n. 131

del 2020. In quella sede, infatti, è stato previsto (articolo 10 del richiamato regolamento), nelle more dell'adozione del presente decreto, che l'elencazione dei soggetti inclusi nel perimetro e gli elenchi dei beni ICT, comprensivi della descrizione dell'architettura e componentistica, nonché dell'analisi del rischio, fossero trattati, conservati e trasmessi con modalità idonee a garantirne la sicurezza, mediante misure tecniche e organizzative adeguate, fatta salva l'eventuale attribuzione di classifiche di segretezza ai sensi dell'articolo 42 della legge n. 124 del 2007.

A tali tipologie di informazioni sono state altresì aggiunte quelle attinenti alle notifiche effettuante ai sensi dell'articolo 3, al modello di cui all'articolo 8 e alla documentazione relativa alle misure di sicurezza di cui all'allegato B, adottate ai sensi degli articoli 7 e 8.

Le misure sono state suddivise in due macro-categorie, la prima relativa ai trattamenti svolti con l'ausilio di strumenti elettronici, la seconda relativa a misure di sicurezza fisica e documentale e rientrano nell'ambito delle categorie di cui all'articolo 1, comma 3, lettera *b)*, numeri 3 e 4, del decreto-legge, relative alla protezione fisica e logica e dei dati (numero 3) e all'integrità delle reti e dei sistemi informativi (numero 4).

Per tali misure – che definiscono un livello minimo di tutela delle informazioni – sono previsti termini più brevi di adozione rispetto a quelli previsti per le misure di sicurezza di cui all'allegato B. Nello specifico, in ragione della necessità di garantire in tempi rapidi la tutela delle predette informazioni, che dovranno essere trattate fin dalla fase iniziale dell'operatività delle misure attuative del decreto-legge, e tenuto conto della tipologia di misure prescritte, che non richiedono particolari interventi da parte dei soggetti tenuti al loro rispetto, è previsto che le stesse debbano essere applicate entro sessanta giorni dalla data di entrata in vigore del presente decreto. È, inoltre, precisato che resta ferma l'adozione da parte dei soggetti inclusi nel perimetro dell'ulteriore e più elevato livello di sicurezza delle misure di cui all'allegato B.

Infine, fermo restando quanto previsto dagli articoli 6 e 10, in relazione alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, in via ricognitiva, viene chiarito che, nel caso in cui alle informazioni, relative a uno degli ambiti oggetto dell'applicazione delle misure minime di cui all'allegato C, venga attribuita una classifica di segretezza ai sensi dell'articolo 42 della legge n. 124 del 2007, troverà applicazione la disciplina recata dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

L'**articolo 10**, per le stesse ragioni di cui all'articolo 6, e in particolare in ragione dell'esclusione dall'elenco dei beni ICT delle reti, dei sistemi informativi e dei servizi informatici attinenti alla gestione delle informazioni classificate disposta dall'articolo 1, comma 2, lettera *b*), del decreto-legge, per ragioni di chiarezza ordinamentale, viene precisato in via ricognitiva, che a tali reti, sistemi informativi

e servizi informatici non si applicano le misure di sicurezza previste dal presente decreto. Viene, quindi, confermato, anche in tale ambito, che 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.

L'**articolo 11**, infine, in aderenza al vincolo di spesa posto dal legislatore, indica che dal presente decreto non derivano nuovi o maggiori oneri per la finanza pubblica.

Per l'illustrazione dei contenuti degli allegati A, B e C, si rinvia a quanto illustrato nell'ambito, rispettivamente, degli articoli 2, 7 e 9.

RELAZIONE TECNICA

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", ha istituito il perimetro di sicurezza nazionale cibernetica al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dei soggetti pubblici e degli operatori economici privati che espletano funzioni essenziali per lo Stato o che prestano servizi essenziali 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. Con il medesimo decreto-legge, inoltre, sono state introdotte disposizioni volte a rafforzare il quadro normativo in tema di esercizio dei poteri speciali nei settori di rilevanza strategica.

Il presente decreto del Presidente del Consiglio dei ministri interviene nel quadro normativo sin qui delineatosi con il decreto-legge e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, ed è adottato in attuazione dell'articolo 1, comma 3, del decreto-legge, su proposta del CISR.

Nello specifico, il presente decreto disciplina, regolandone, altresì, i relativi termini e le modalità attuative:

- ai sensi dell'articolo 1, comma 3, lettera *a*), le procedure con cui i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, individuati nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del decreto-legge, notificano al CSIRT italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b*) del decreto-legge (nelle definizioni del presente decreto indicati come "beni ICT");
- ai sensi dell'articolo 1, comma 3, lettera *b*), le misure volte a garantire elevati livelli di sicurezza dei beni ICT, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

In relazione a tanto, il presente decreto prevede due tipologie di obblighi che, come si illustrerà, non comportano nuovi o maggiori oneri per la finanza pubblica: obblighi di notifica e obblighi di adozione delle misure di sicurezza.

In particolare, per quanto concerne gli obblighi di notifica, il decreto impone di notificare, tramite appositi canali di comunicazione del CSIRT italiano, gli incidenti che abbiano impatto su un bene ICT. Ciò, anche nell'ipotesi in cui gli stessi incidenti,

che abbiano impatto su un bene ICT, si verifichino a carico di un bene, sistema informativo o servizio informatico non incluso nel predetto elenco, ma che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o di memoria ovvero software di base. Prescrive, inoltre, un dovere di integrazione della notifica nel caso in cui il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi.

All'adempimento dei suddetti obblighi di notifica, i soggetti pubblici inclusi nel perimetro provvedono nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Con riferimento alla seconda tipologia di obblighi, il decreto dispone che i soggetti inclusi nel perimetro, adottino, per ciascun bene ICT di rispettiva pertinenza, le misure di sicurezza individuate nell'allegato B al presente decreto e corrispondenti agli ambiti indicati all'articolo 1, comma 3, lettera *b*), del decreto-legge, comunicandone l'avvenuta adozione e le relative modalità mediante il modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano. È inoltre previsto che i soggetti tenuti all'adozione delle misure di sicurezza debbano adeguare le stesse ogniqualvolta dovessero ritenerlo necessario a seguito di aggiornamenti occorsi sull'elenco dei beni ICT.

In relazione a tali oneri, si provvederà, come è stato precisato anche nella relazione tecnica allegata al decreto-legge, positivamente verificata dalla Ragioneria Generale dello Stato, a decorrere dagli esercizi finanziari 2020/2021, con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente.

Per quanto concerne la mancanza di impatto sulla finanza pubblica in ordine all'eventuale adeguamento alle misure di sicurezza, si richiama l'articolo 1, comma 18, del decreto-legge, il quale precisa, infatti, che gli eventuali adeguamenti alle prescrizioni di sicurezza sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

Sia in relazione alla modalità di trasmissione delle notifiche di incidente, che in riferimento allo strumento da utilizzare per la comunicazione in ordine all'avvenuta adozione delle misure di sicurezza e dei relativi aggiornamenti, il decreto prevede che vengano utilizzati gli appositi canali di comunicazione del CSIRT italiano.

In primo luogo, è previsto che la notifica avvenga tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera a), dell'allegato I, del decreto legislativo 18 maggio 2018 n. 65, secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet dello stesso CSIRT italiano, già reso operativo. Il ricorso a tali canali di comunicazione, in quanto relativi al CSIRT italiano, già istituito presso il DIS con il decreto legislativo n. 65 del 2018 e successivamente disciplinato con il decreto del Presidente del Consiglio dei ministri 8

agosto 2019, non comporta nuovi oneri o maggiori per la finanza pubblica, atteso che all'implementazione dei suddetti canali si provvederà con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI di cui all'articolo 29 della legge 3 agosto 2007, n. 124, già disponibili.

In secondo luogo, è previsto che l'avvenuta adozione delle misure di sicurezza, comprensiva delle relative modalità, venga comunicata dal soggetto incluso nel perimetro mediante la piattaforma digitale costituita presso il DIS, ai sensi del regolamento adottato con il DPCM n. 131 del 2020, con il modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano. L'utilizzo della piattaforma digitale, come indicato nella relazione tecnica al citato regolamento adottato con DPCM n. 131 del 2020, non comporta nuovi oneri a carico della finanza pubblica, poiché al funzionamento della piattaforma istituita presso il DIS, si provvede con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI di cui al citato articolo 29 della legge 3 agosto 2007, n. 124, già disponibili. Per quanto concerne l'utilizzo del modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano, alla luce delle argomentazioni sopra riportate, non si ravvisa un impatto sulla finanza pubblica.

Sempre in relazione agli obblighi di adozione delle misure di sicurezza, il presente decreto individua, infine, misure di sicurezza minime, di natura tecnica e organizzativa, che i soggetti inclusi nel perimetro sono tenuti ad applicare per tutelare le informazioni relative: all'elencazione dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge; all'elenco dei beni ICT di cui all' all'articolo 1, comma 2, lettera *b*), del decreto-legge; agli elementi delle notifiche di incidente, di cui all'articolo 3 del presente decreto; al modello, infine, con cui viene comunicata l'adozione, e le relative modalità, delle misure di sicurezza da applicarsi sui beni ICT, di cui all'articolo 8 del presente decreto. Anche in relazione a tali oneri, si provvederà, a decorrere dagli esercizi finanziari 2020/2021, con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente, così come sopra precisato con riferimento agli oneri derivanti dall'adozione delle misure di sicurezza sui beni ICT.

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

IL CAPO DEL DIPARTIMENTO

Visto l'articolo 6, comma 1, lettera c), del decreto del Presidente del Consiglio dei ministri 15 settembre 2017, n. 169, che dispone l'esclusione dell'AIR per i provvedimenti normativi concernenti "disposizioni direttamente incidenti su interessi fondamentali in materia di sicurezza interna ed esterna dello Stato";

Considerato che lo schema di decreto del Presidente del Consiglio dei ministri, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione dell'articolo 1, comma 3, del medesimo decreto-legge 21 settembre 2019, n. 105, concerne disposizioni necessarie per la sicurezza interna dello Stato;

DICHIARA

l'esclusione dall'AIR per lo schema di decreto del Presidente del Consiglio dei ministri, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione dell'articolo 1, comma 3, del medesimo decreto-legge 21 settembre 2019, n. 105.

Roma,

Pres. Ermanno de Francisco

ROMA 2009 - ISTITUTO POLIGRAFICO E ZECCA DELLO STATO S.p.A. - 3.

ANALISI TECNICO-NORMATIVA

Titolo: Schema di decreto del Presidente del Consiglio dei ministri, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Amministrazione referente: Presidenza del Consiglio dei ministri.

PARTE I - ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.

Il decreto del Presidente del Consiglio dei ministri è adottato in attuazione dell'articolo 1, comma 3, del 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 (nel prosieguo "decreto-legge").

Nello specifico, nel provvedere a regolare, altresì, i relativi termini e le modalità attuative, lo schema di decreto:

- disciplina, ai sensi dell'articolo 1, comma 3, lettera *a*), del decreto-legge, le procedure con cui i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, individuati nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del decreto-legge, notificano al CSIRT italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge (nelle definizioni del presente decreto indicati come "beni ICT");
- stabilisce, ai sensi dell'articolo 1, comma 3, lettera *b*), del decreto-legge, le misure volte a garantire elevati livelli di sicurezza dei beni ICT, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

Il presente schema di decreto è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica, sulla base della procedura prevista all'articolo 1, commi 3 e 4-*bis,* del decreto-legge, che dispone la previa trasmissione del testo alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, nonché al Comitato parlamentare per la sicurezza della Repubblica. Poiché la proposta di decreto ha evidenziato indici che hanno indotto a ritenerne il carattere normativo, lo schema viene inoltre sottoposto al parere del Consiglio di Stato.

Il presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, è inoltre soggetto ad aggiornamento periodico, con cadenza almeno biennale, con le medesime modalità seguite per la sua adozione.

Trattandosi di intervento attuativo del decreto-legge, l'adozione del presente decreto risulta necessaria al fine di assicurare la concreta operatività degli obblighi di notifica e di adozione delle misure di sicurezza sottesi all'istituzione del perimetro di sicurezza nazionale cibernetica ed è coerente con l'impegno del Governo di adottare, accanto alle azioni dirette ad accrescere la digitalizzazione del Paese – fattore imprescindibile di sviluppo e di crescita – tutte le misure necessarie per assicurare elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale.

2) Analisi del quadro normativo nazionale.

Il presente decreto attuativo si innesta nel quadro normativo sin qui delineatosi con il decreto-legge in tema di sicurezza nazionale cibernetica e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, disciplinando, pertanto, nella prospettiva della tutela della sicurezza nazionale, le misure necessarie ad assicurare elevati livelli di sicurezza informatica di reti, sistemi informativi e servizi informatici 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 o interruzione, anche parziali, ovvero utilizzo improprio, possano derivare pregiudizi per la sicurezza nazionale.

Vengono, a tal fine, definite le procedure per la notifica degli incidenti aventi impatto sui beni ICT, e individuate le misure di sicurezza da applicarsi sui beni ICT.

Nello specifico, il quadro normativo in cui interviene il presente decreto di attuazione è delineato dai seguenti provvedimenti:

- la legge 3 agosto 2007, n. 124, recante l'istituzione del Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto, che all'articolo 1, comma 3-*bis,* dispone che il Presidente del Consiglio dei ministri impartisce al Dipartimento delle informazioni per la sicurezza (DIS) e ai Servizi di informazione per la sicurezza direttive per rafforzare la protezione cibernetica e la sicurezza informatica nazionali e all'articolo 4, comma 3, lettera d-*bis*), attribuisce al DIS il compito di coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;
- il decreto legislativo 15 settembre 2003, n. 259 (di seguito "codice delle comunicazioni elettroniche"), che, all'articolo 16-*bis,* prevede l'obbligo per le imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico di adottare misure di natura tecnica e organizzativa volte a garantire la sicurezza delle reti e dei servizi di

comunicazione elettronica accessibili al pubblico, nonché di comunicare al Ministero dello sviluppo economico ogni significativa violazione della sicurezza o perdita dell'integrità delle reti. In attuazione del citato articolo 16-*bis* e dell'articolo 16-*ter* del codice delle comunicazioni elettroniche è stato adottato il decreto del Ministro dello sviluppo economico 12 dicembre 2018, che ha individuato adeguate misure di natura tecnico-organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente, e ha definito i casi in cui le violazioni della rete o la perdita dell'integrità sono da considerarsi significative ai fini della notifica al CSIRT italiano e ad altre competenti Autorità;

- il decreto legislativo 18 maggio 2018, n. 65 - di seguito "decreto legislativo NIS", di recepimento della direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva "NIS"), che, nell'individuare le misure volte a conseguire un livello elevato di sicurezza delle reti e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea, agli articoli 12 e 14 prevede obblighi di adozione di misure tecniche e organizzative in capo agli operatori di servizi essenziali e ai fornitori di servizi digitali per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali e dei servizi digitali, nonché obblighi di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. Il citato decreto legislativo, inoltre, all'articolo 8, istituisce presso la Presidenza del Consiglio dei ministri, ed in particolare presso il DIS, il CSIRT italiano, a cui è attribuito il compito di svolgere le funzioni del *computer emergency response team* (CERT) nazionale, di cui all'articolo 16-*bis* del codice delle comunicazioni elettroniche e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo n. 82 del 2005, nonché le funzioni di cui all'allegato I, punto 2, del decreto legislativo n. 65 del 2018;
- il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" all'articolo 3, comma 1, lettera *b*), ha previsto che il Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la sicurezza della Repubblica, adotti il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (la cui adozione è stata successivamente prevista, a livello primario, dal decreto legislativo NIS, all'articolo 6 del decreto legislativo n. 65 del 2018), nell'ambito del quale è stato richiesto il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese. In attuazione dell'articolo 3, comma 1, lettera *c*), da ultimo con decreto del Presidente del Consiglio dei ministri 31 marzo 2017, è stato adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica. In attuazione dell'articolo 11, comma 2, del citato DPCM 17 febbraio 2017, con decreto del Ministro dello sviluppo economico del 15 febbraio 2019, è stato istituito, presso l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, il Centro di valutazione e certificazione nazionale (CVCN), che, in ambito perimetro, è chiamato a svolgere le sue funzioni istituzionali di

verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici inclusi nell'elenco dei beni ICT, al fine di rendere il relativo approvvigionamento più sicuro;

- il decreto del Presidente del Consiglio dei ministri 26 settembre 2019, con cui sono state delegate al Ministro per l'innovazione tecnologica e la digitalizzazione le funzioni spettanti al Presidente del Consiglio dei ministri in materia di innovazione digitale, all'articolo 1, comma 3, lettera *c*), ha, in particolare, delegato al predetto Ministro le funzioni e i compiti demandati alla Presidenza del Consiglio dei ministri ai fini della attuazione del decreto-legge;
- da ultimo, il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, in attuazione dell'articolo 1, comma 2, del decreto-legge, pubblicato nella *Gazzetta Ufficiale* n. 261, del 21 ottobre 2020. Con tale provvedimento sono state definite le modalità e i criteri procedurali di individuazione dei soggetti da includere nel perimetro di sicurezza nazionale cibernetica e sono stati individuati i criteri con i quali tali soggetti predispongono e aggiornano l'elenco dei beni ICT;

3) Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.

Il presente decreto, come anticipato, si muove lungo le direttrici dispositive tracciate dal decreto-legge, attuando le previsioni ivi contenute.
A tal riguardo, il decreto-legge, all'articolo 1, comma 8, ha introdotto delle disposizioni volte a coordinare gli obblighi che discendono dall'inclusione dei soggetti nel perimetro di sicurezza nazionale cibernetica con quelli derivanti in capo ai medesimi soggetti:
- dal decreto legislativo NIS, circa l'obbligo di notificare gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti e di adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi;
- dal codice delle comunicazioni elettroniche e delle correlate disposizioni attuative, relativi all'obbligo di comunicare ogni significativa violazione della sicurezza o perdita dell'integrità delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e di adottare adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle stesse reti.

Nello specifico, il decreto-legge ha previsto che l'assolvimento dell'obbligo di notifica ai sensi dell'articolo 1, comma 3, lettera *a*), del decreto-legge degli obblighi di notifica previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche. Conseguentemente, lo schema di decreto ha provveduto a specificare che, qualora l'incidente rilevi anche ai fini del decreto legislativo NIS, ovvero del codice delle comunicazioni elettroniche, nell'effettuare la notifica al CSIRT italiano, indicano rispettivamente l'autorità competente NIS (alla quale il CSIRT italiano provvederà ad inoltrare la notifica). In via meramente ricognitiva, viene, inoltre, precisato che restano fermi gli obblighi di notifica, secondo le relative procedure, previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche e relative disposizioni

attuative per quegli incidenti che non rientrano nell'ambito di applicazione del decreto-legge.

Con riferimento alle misure di sicurezza, il decreto-legge ha stabilito che i soggetti inclusi nel perimetro osservano le misure di sicurezza previste dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche, ove di livello almeno equivalente a quelle adottate ai sensi dell'articolo 1, comma 3, lettera *b*), del decreto-legge, facendo salva, tuttavia, la possibilità da parte della Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, e del Ministero dello sviluppo economico, per i soggetti privati, di individuare eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal decreto-legge.

4) Analisi della compatibilità dell'intervento con i principi costituzionali

Il provvedimento è stato predisposto nel rispetto dei principi costituzionali.

5) Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Il decreto non presenta aspetti di interferenza o di incompatibilità con le competenze costituzionali delle Regioni poiché incide sulla materia "sicurezza dello Stato", riservata alla competenza legislativa esclusiva dello Stato ai sensi dell'art. 117, comma 2, lettera *d*), della Costituzione. In virtù del parallelismo tra competenza legislativa esclusiva e potestà regolamentare, sancita dall'art. 117, comma 6, della Costituzione, la potestà regolamentare in materia di perimetro di sicurezza nazionale cibernetica spetta allo Stato.

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Non si ravvisano elementi di incompatibilità.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

Trattandosi di intervento normativo di tipo attuativo, vertente peraltro su una tematica (perimetro di sicurezza nazionale cibernetica) sulla quale antecedentemente all'entrata in vigore del decreto-legge non si è legiferato, si esclude che il presente decreto possa costituire una rilegificazione, ovvero che possa qualificarsi quale intervento di delegificazione.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Non vi sono elementi da segnalare.

9) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

PARTE II - CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

1) Analisi della compatibilità dell'intervento con l'ordinamento comunitario

Non si ravvisano elementi di incompatibilità, poiché, ai sensi dell'articolo 4, paragrafo 2, del Trattato sull'Unione europea, la materia della "sicurezza nazionale" resta di esclusiva competenza di ciascuno Stato membro.
Con l'intervento in esame viene data attuazione ad una disciplina – quella contenuta nel decreto-legge – che appare complementare rispetto al quadro ordinamentale introdotto con la 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 – recepita nell'ordinamento interno con il decreto legislativo 18 maggio 2018, n. 65 – poiché vengono stabiliti, per finalità di sicurezza nazionale, gli adempimenti attuativi necessari a garantire i nuovi e più elevati livelli di tutela e di sicurezza delle reti, sistemi informativi e servizi informatici introdotti dal decreto-legge. Analoghe considerazioni valgono anche per quanto riguarda la compatibilità del presente decreto con il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. "Cybersecurity Act").

2) Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Non risultano procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

3) Analisi della compatibilità dell'intervento con gli obblighi internazionali.

Il provvedimento non presenta profili di incompatibilità con gli obblighi internazionali.

4) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non risultano pendenti giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

5) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

6) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Non vi sono elementi da segnalare.

PARTE III - ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

L'articolo 1 dello schema di decreto mutua la maggior parte delle definizioni, per esigenze di coerenza, dal regolamento adottato con il DPCM n. 131 del 2020, in attuazione dell'articolo 1, comma 2, del decreto-legge, e al contempo riformula alcune delle definizioni ivi recate al fine di tenere conto dell'avvenuta adozione del richiamato regolamento, e introduce altre mirate definizioni ritenute rilevanti ai fini della elaborazione dei contenuti del presente decreto.

Nello specifico, rispetto al citato regolamento, è stata adeguata la definizione di "*bene ICT*", già recata dal DPCM n. 131 del 2020, al fine di tenere conto dell'inserimento, da parte di ciascuno dei soggetti inclusi nel perimetro, dei beni ICT nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge. Sono state introdotte, poi, le definizioni di "*soggetti inclusi nel perimetro*", al fine di dare conto dell'avvenuta inclusione dei soggetti di cui all'articolo 1, comma 2, lettera *a*), del decreto-legge, nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge, e di "*impatto sul bene ICT*", al fine di individuare l'ambito di operatività della disposizione di cui all'articolo 1, comma 3, lett. *a*), del decreto-legge che impone l'obbligo di notifica al CSIRT italiano degli incidenti "*aventi impatto sui beni ICT*".

2) Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni ed integrazioni subite dai medesimi.

Lo schema di decreto del Presidente del Consiglio dei ministri fa corretto riferimento alla legislazione nazionale vigente.

3) Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.

Non vi sono elementi da segnalare.

4) Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.

Non vi sono elementi da segnalare.

5) Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

Non vi sono elementi da segnalare.

6) Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.

Non vi sono elementi da segnalare.

7) Indicazione degli eventuali atti successivi attuativi, verifica della congruenza dei termini previsti per la loro adozione.

Il presente decreto non prevede successivi atti attuativi. La tassonomia degli incidenti di cui all'articolo 2, le misure di sicurezza da applicare per ciascun bene ICT di cui all'articolo 7 e le misure di sicurezza minime per la tutela delle informazioni di cui all'articolo 9 sono puntualmente indicate, rispettivamente, negli allegati A, B e C del presente decreto.

8) Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.

Per la predisposizione dell'intervento normativo sono stati considerati i dati in possesso delle Amministrazioni coinvolte nell'attuazione delle disposizioni del decreto-legge.

Numero 00028/2021 e data 11/01/2021 Spedizione

REPUBBLICA ITALIANA

Consiglio di Stato

Sezione Consultiva per gli Atti Normativi

Adunanza di Sezione del 1 dicembre 2020

NUMERO AFFARE 01357/2020

OGGETTO:

Presidenza del consiglio dei ministri - Dipartimento per gli affari giuridici e legislativi.

Schema di decreto del Presidente del consiglio dei ministri, recante "*Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

LA SEZIONE

Vista la nota di trasmissione n. prot. 11356 del 18 settembre 2020 con la quale la Presidenza del Consiglio dei ministri - Dipartimento per gli affari giuridici e

legislativi ha trasmesso lo schema di decreto del Presidente del consiglio dei ministri, recante "*Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

Esaminati gli atti e udito il relatore, consigliere Paolo Carpentieri;

Premesso:

1. Il decreto-legge 21 settembre 2019, n. 105, recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ha istituito, nell'art. 1, il *perimetro di sicurezza nazionale cibernetica*, al fine di *assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.*

2. Lo schema di decreto in esame attua in particolare le previsioni del comma 3 dell'articolo 1 citato, che demanda a un apposito decreto del Presidente del consiglio dei ministri, da adottarsi su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, la definizione (con annessa disciplina dei termini e delle modalità attuative): a) delle procedure in base alle quali i

soggetti inclusi nel perimetro di sicurezza nazionale cibernetica notificano al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nel perimetro; b) delle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici suddetti, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea riguardo ai seguenti settori di attività e profili (definiti anche "*ambiti*" nell'ultimo *Considerato* del preambolo dello schema di decreto, nella relazione illustrativa e nell'articolo 7, comma 1): struttura organizzativa preposta alla gestione della sicurezza, politiche di sicurezza, gestione del rischio, mitigazione e gestione degli incidenti e loro prevenzione, protezione fisica e logica e dei dati, integrità delle reti e dei sistemi informativi, gestione operativa, monitoraggio, test e controllo, formazione e consapevolezza, affidamento di forniture di beni, sistemi e servizi ICT.

3. Lo schema di decreto si compone complessivamente di 11 articoli ed è suddiviso in quattro Capi. Il Capo I è dedicato alle "*Disposizioni generali*", il Capo II alle "*Notifiche di incidente*", il Capo III alle "*Misure di sicurezza*" e il Capo IV alle "*Disposizioni finali*". Le "*Disposizioni generali*" si risolvono nel solo articolo 1, recante le definizioni (correttamente concordanti con quelle della legge e con quelle già previste nei precedenti, citati, decreti attuativi). Il Capo II, sulle *Notifiche di incidente*, comprende gli articoli 2 (*Tassonomia degli incidenti*), 3 (*Notifica degli incidenti aventi impatto su beni ICT*), 4 (*Notifica volontaria degli incidenti*), 5 (*Trasmissione delle notifiche*) e 6 (*Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*). Il Capo III riguarda le "*Misure di sicurezza*" e comprende gli articoli 7 (*Misure di sicurezza*), 8 (*Modalità e termini di adozione delle misure di sicurezza*), 9 (*Tutela delle informazioni*) e 10 (*Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*). Il Capo IV ("*Disposizioni finali*") è costituito dal solo articolo 11 (*Disposizioni finali*) che si risolve nella clausola di invarianza della spesa.

4. L'articolato è completato da tre allegati: l'allegato A, previsto dall'articolo 2, che reca la tassonomia degli incidenti; l'allegato B, previsto dall'articolo 7, che reca le misure di sicurezza (con due appendici: l'appendice n. 1, costituita da una tabella di corrispondenza tra gli ambiti di cui all'articolo 1, comma 3, lettera *b*), del decreto-legge e le misure di sicurezza dell'allegato B, nonché l'appendice n. 2, costituita da una tabella di corrispondenza tra le misure di sicurezza e le categorie A - B); l'allegato C, previsto dall'articolo 9, che reca le misure minime di sicurezza per la tutela delle informazioni.

5. Il testo è corredato di relazione tecnica, di analisi tecnico-normativa (ATN), di stralcio del verbale del Comitato interministeriale per la sicurezza della Repubblica - CISR del 27 ottobre 2020. Il testo non è invece corredato di analisi di impatto della regolazione (AIR) poiché ne è richiesta l'esclusione, ai sensi dell'articolo 6, comma 1, del d.P.C.M. n. 169 del 2017 (con nota del Capo del Dipartimento per gli affari giuridici e legislativi), con la motivazione che "*il provvedimento in esame concerne misure necessarie per la sicurezza interna dello Stato*".

6. La relazione illustrativa informa, circa l'*iter* elaborativo del testo, che sono stati costituiti appositi gruppi di lavoro, che hanno visto la partecipazione dei rappresentanti delle diverse amministrazioni interessate, e che la condivisione tra le amministrazioni sulle diverse soluzioni tecnico-giuridiche elaborate e, quindi, sullo schema di decreto è stata, poi, assicurata nell'ambito dell'organismo tecnico di supporto al CISR di cui all'articolo 4, comma 5, del regolamento adottato con d.P.C.M. 3 aprile 2020, n. 2 (il c.d. "CISR tecnico"), integrato da un rappresentante della struttura della Presidenza del Consiglio competente per la innovazione tecnologica e la digitalizzazione, designato in ragione degli specifici compiti attribuiti alla Presidenza del consiglio dal decreto-legge, nonché da rappresentanti del Ministero delle infrastrutture e dei trasporti, del Ministero del lavoro e delle politiche sociali, del Ministero dell'università e ricerca, nonché dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri. Sullo schema di

decreto è infine intervenuto il CISR - organo al quale compete la proposta di adozione - che ha favorevolmente deliberato sul testo, in via preliminare, nella seduta del 27 ottobre 2020.

Considerato:

I. Considerazioni generali

1. La norma primaria (art. 1, comma 3, del decreto-legge n. 105 del 2019) prevede che il decreto attuativo ivi previsto debba essere adottato "*Entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto*" (ossia entro dieci mesi dal 21 novembre 2019, data di entrata in vigore della legge di conversione 18 novembre 2019, n. 133). Il termine sarebbe dunque venuto a scadenza il 21 ottobre 2020. Tuttavia l'articolo 103, comma 1, del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, ha stabilito che "*Ai fini del computo dei termini ordinatori o perentori, propedeutici, endoprocedimentali, finali ed esecutivi, relativi allo svolgimento di procedimenti amministrativi su istanza di parte o d'ufficio, pendenti alla data del 23 febbraio 2020 o iniziati successivamente a tale data, non si tiene conto del periodo compreso tra la medesima data e quella del 15 aprile 2020*". Successivamente, l'articolo 37 del decreto-legge legge 8 aprile 2020, n. 23, convertito, con modificazioni, dalla legge 5 giugno 2020, n. 40, ha prorogato il suddetto termine al 15 maggio 2020. Il Collegio ritiene che tale periodo di sospensione sia applicabile anche al termine per l'adozione dei regolamenti. Ne consegue che il termine ultimo utile per l'adozione del decreto in esame deve ritenersi prorogato *ex lege* di 81 giorni (pari al periodo di sospensione, dal 23 febbraio al 15 maggio 2020).

2. Il Collegio rileva che molti degli "incidenti" rilevanti contemplati dal presente schema di decreto rientrerebbero nell'ambito della casistica di violazione dei dati personali ("*Data Breach*") soggetta a notifica all'autorità di controllo ai sensi dell'articolo 33 del "Gdpr" [*Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con*

riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)]. Sarebbe stato dunque necessario acquisire il parere del Garante per la protezione dei dati personali. Rileva tuttavia il Collegio che il Gdpr esclude dal suo ambito di applicazione, nell'articolo 2, paragrafo 2, i trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quelli effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE (*Disposizioni specifiche sulla politica estera e di sicurezza comune*), nonché quelli effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. Sarebbe necessario che l'Amministrazione chiarisse, almeno nella relazione illustrativa, se e quali di tali ragioni rilevino nel caso in esame al fine di giustificare la mancata acquisizione del suddetto parere.

3. La Sezione ha già avuto occasione di recente di occuparsi della tematica degli strumenti attuativi dell'articolo 1 del decreto-legge n. 105 del 2019 in materia di perimetro di sicurezza nazionale cibernetica, pronunciandosi dapprima (con il parere n. 983 del 26 maggio 2020) sullo schema di decreto del Presidente del Consiglio dei ministri adottato in attuazione dell'articolo 1, comma 2, del predetto decreto-legge per la definizione degli ambiti soggettivi e oggettivi inclusi nel perimetro di sicurezza nazionale cibernetica e dei criteri di predisposizione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici (d.P.C.M. 30 luglio 2020, n. 131); quindi (con il parere 26 ottobre 2020, n. 1664) sullo schema di decreto del Presidente della Repubblica attuativo dell'articolo 1, comma 6, del decreto-legge n. 105 del 2019, di disciplina delle procedure, delle modalità e dei termini per le verifiche e i controlli sugli acquisti di beni e servizi ICT compresi nel perimetro (regolamento, quest'ultimo, a quel che

consta, non ancora adottato).

4. Sulla notevole complessità del quadro normativo introdotto dall'articolo 1 del decreto-legge n. 105 del 2019 – e sulla conseguente necessità di ricondurre a unità, per quanto possibile, le plurime fonti normative attuative in esso previste – la Sezione si è già espressa e non può, sul punto, che rinviarsi a quanto esplicitato nei citati, precedenti pareri vertenti su questa tematica.

5. La materia trattata – in specie per quanto attiene agli allegati – presenta un alto tasso di tecnicismo, implicante il responsabile esercizio di delicate valutazioni di discrezionalità tecnica, che non possono che essere rimesse e riservate all'Amministrazione. Il presente parere si occuperà, dunque, soprattutto (se non esclusivamente) dei profili giuridico-formali di maggiore evidenza e rilievo.

II. Esame dell'articolato.

1. Articolo 1 (*Definizioni*)

1.1. Non si hanno osservazioni da formulare, salve le eventuali integrazioni indicate nei successivi paragrafi 3.3 e 3.4.

2. Articolo 2 (*Tassonomia degli incidenti*)

2.1. Il testo del comma 1 presenta una formulazione non molto lineare. Si suggerisce la seguente riformulazione: "*Nelle tabelle n. 1 e n. 2 dell'allegato A al presente regolamento sono classificati 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*".

2.2. Le tabelle (nn. 1 e 2) contenute nell'allegato A sono costituite ciascuna da tre colonne recanti, nella prima colonna a sinistra, un codice identificativo (ICP-A-2, ICP-A-3, ICP-A-4 e così a seguire in ordine crescente nella tabella A; ICP-B-2, ICP-B-3, ICP-B-4, *etc*., nella tabella B); in quella centrale la categoria di incidente [*Infezione (Initial exploitation), Guasto (Fault), Installazione (Establish persistence)*, *etc*.] e nella colonna di destra una descrizione della consistenza di ciascuna specie di incidente (corrispondente al codice identificativo) rientrante

nelle diverse categorie. Sarebbe molto utile, a giudizio della Sezione, che nell'articolo 2 fosse inserito un adeguato riferimento esplicativo di rinvio alla suddetta classificazione delle diverse tipologie di incidenti, idoneo a chiarificarne la struttura logica. È inoltre necessario, almeno in calce (o in testa) alle tabelle, definire l'acronimo "ICP" del codice identificativo.

3. Articolo 3 (*Notifica degli incidenti aventi impatto su beni ICT*).

3.1. Comma 2. Come risulta bene chiarito nella relazione tecnica, il decreto impone di notificare, tramite appositi canali di comunicazione del CSIRT italiano, gli incidenti che abbiano impatto su un bene ICT, e "*ciò, anche nell'ipotesi in cui gli stessi incidenti, che abbiano impatto su un bene ICT, si verifichino a carico di un bene, sistema informativo o servizio informatico non incluso nel predetto elenco, ma che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o di memoria ovvero software di base*". Questo obbligo risulta invece declinato in modo poco chiaro nel testo del comma 2 dell'articolo 3 in esame, che deve essere riformulato come segue: "*I soggetti inclusi nel perimetro procedono alla notifica di cui al comma 1 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 condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione*".

3.2. Il comma 3, per analoghe esigenze di qualità del testo normativo, deve essere riformulato come segue: "*La notifica deve essere effettuata entro sei ore dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 1 di cui all'allegato A ed entro un'ora nel caso di incidenti individuati nella tabella 2 di cui all'allegato medesimo. 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".

3.3. Nel comma 4, relativo all'obbligo di comunicazione degli ulteriori elementi informativi emersi sulla natura, la dinamica, gli effetti dell'incidente, l'avverbio "*tempestivamente*" – in sé privo di un utile significato normativo – deve essere sostituito con l'avverbio "*immediatamente*". Conseguentemente la frase "*dal momento in cui il soggetto incluso nel perimetro ne è venuto a conoscenza*" (al quarto e quinto rigo del comma) può essere eliminata perché ridondante. Se si intende fare uso della sigla "*IOC*" occorre fornirne un'apposita definizione nell'articolo 1.

3.4. Nel comma 5, attuativo del comma 8 dell'articolo 1 del decreto-legge n. 105 del 2019, si prevede l'obbligo di comunicazione della notifica alla "*autorità competente NIS*" ai sensi del decreto legislativo n. 65 del 2018. La "*autorità competente NIS*" – definita dall'articolo 3 del decreto legislativo n. 65 del 2018 (1. *Ai fini del presente decreto si intende per: a) autorità competente NIS, l'autorità competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1*") – non risulta invece definita nell'articolo 1 del presente schema di decreto. Occorrerà, pertanto, in alternativa, o integrare l'elenco delle definizioni dell'articolo 1 (con un rinvio alla norma primaria ora citata), o inserire tale rinvio nel testo del comma 5 in esame.

3.5. Il comma 8 prevede che "*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*". La disposizione intende evidentemente stabilire che della notifica dell'incidente sia informata la struttura di *cybersecurity* interna al soggetto (incluso nel perimetro) che ha subito l'incidente (e che ha quindi effettuato la notifica). La formulazione del comma è tuttavia poco chiara. La voce (*categoria*) 2.1 dell'allegato B riguarda, nell'ambito delle misure di sicurezza, le modalità di organizzazione e gestione delle apposite strutture (dei soggetti ricompresi nel perimetro) di "*Gestione degli asset (Asset Management) (ID.AM)*", finalizzate ad

assicurare – come precisato nell'allegato citato - che "*i dati, il personale, i dispositivi, i sistemi e le facility necessari all'organizzazione siano identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione*". Più in particolare la voce (sottocategoria) 2.1.4 (ID.AM-6) riguarda la definizione dei ruoli e delle responsabilità inerenti la *cybersecurity* per tutto il personale e per eventuali terze parti rilevanti (fornitori, clienti, *partner*). Ciò chiarito, occorre che il testo del comma in esame sia riformulato con una più esplicita e diretta indicazione dell'oggetto cui essa riferisce, alla quale potrà aggiungersi anche il rinvio alla corrispondente voce dell'allegato 2, non essendo sufficiente la mera indicazione del codice identificativo di tale voce (categoria e sottocategoria identificative della misura di sicurezza).

4. Articolo 4 (*Notifica volontaria degli incidenti*).

4.1. Occorre chiarire se la "*notifica volontaria*" debba essere effettuata attraverso gli stessi canali dedicati previsti per la notifica obbligatoria dall'articolo 3. Valuti inoltre l'Amministrazione se non sia preferibile e opportuno qualificare tale "*notifica volontaria*" con il diverso termine "*informativa volontaria*" o "*comunicazione volontaria*", eventualmente specificando modalità alternative e semplificate di comunicazione, posto che, come esplicitato nel comma 2, nessun obbligo ulteriore può derivare da tale iniziativa in capo al soggetto che effettua la comunicazione.

4.2. Il comma 3 deve essere riformulato nei seguenti, più semplici termini: "*Dalla notifica volontaria non deriva alcun obbligo di ulteriori adempimenti a carico del soggetto notificante*".

4.3. Vale per il comma 4 quanto considerato a proposito dell'articolo 3, comma 8. In alternativa, valuti l'Amministrazione se non riformulare il comma come segue: "*Si applica il comma 8 dell'articolo 3*".

5. Articolo 5 (*Trasmissione delle notifiche*).

5.1. L'articolo 5 attua la disposizione del secondo periodo della lettera *a*), del

comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019, in base alla quale "*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*". Manca, tuttavia, nella sequenza logico-giuridica dell'articolato, così come costruito nello schema di d.P.C.M. in esame, il passaggio precedente e pregiudiziale, previsto nel periodo precedente della medesima lettera *a*) citata, in base al quale il "*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*". È vero che il CISIRT italiano non è che un organismo interno al DIS (istituito ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018). Tuttavia, avendo la legge previsto espressamente questo passaggio (ancorché "interno"), si reputa corretto farne menzione, per completezza, anche nel regolamento. Occorre, dunque, inserire (valuti l'Amministrazione se nell'articolo 5 o precedentemente) una disposizione che attui (o, quanto meno, richiami) il predetto passaggio normativo, chiarendo che il CSIRT italiano (*Computer security incident response team*) trasmette immediatamente al DIS le notifiche ricevute.

5.2. L'alinea del comma 1 deve essere riformulato come segue: "*Il DIS inoltra le notifiche ricevute:*". Nelle lettere *b*) e *c*) la parola "*stesse*" deve essere sostituita con la parola "*notifiche*". Prima dell'attuale comma 2 deve essere quindi aggiunto il seguente comma "2. *Le notifiche volontarie, di cui all'articolo 4, sono trasmesse solo nel caso in cui siano state trattate*". L'attuale comma 2 diviene conseguentemente comma 3.

5.3. Nell'attuale comma 3 (che diventa comma 4) le parole "*per gli inoltri*" devono

essere sostituite dalle seguenti: "*di inoltro*" e le parole "*possono essere concordate*" devono essere sostituite dalle seguenti: "*sono definite*".

6. Articolo 6 (*Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*).

Nessuna osservazione.

7. Articolo 7 (*Misure di sicurezza*).

7.1. L'articolo 7 fornisce una sorta di "legenda" dell'allegato 2, chiarendo che "*Le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere, sono individuate nell'allegato B al presente regolamento*". Nella *Premessa* contenuta nell'allego 2 si chiarisce ulteriormente che "*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*". In proposito la Sezione rimette all'Amministrazione la verifica tecnica dell'adeguata corrispondenza tra le macro-aree di intervento individuate nell'allegato B e i nove "*ambiti*" – cui devono riferirsi le misure di sicurezza - previste espressamente dall'articolo 1, comma 3, lettera *b*), del decreto-legge n. 105 del 2019 (struttura organizzativa preposta alla gestione della sicurezza, alle politiche di sicurezza e gestione del rischio, mitigazione e gestione degli incidenti e loro prevenzione, protezione fisica e logica e dei dati, integrità delle reti e dei sistemi informativi, gestione operativa, ivi compresa la continuità del servizio, monitoraggio, test e controllo, formazione e consapevolezza, affidamento di forniture di beni, sistemi e servizi ICT).

7.2. Sarebbe comunque utile – per una più agevole lettura - una più puntuale denominazione delle rubriche dell'indice dell'allegato 2, in modo da chiarire che le *funzioni* sono costituite dalle "macro-aree" o fasi di rilevazione e reazione rispetto al verificarsi di incidenti definite dai numeri cardinali dei paragrafi (*Identificazione*

- paragrafo 2, *Protezione* – paragrafo 3, *Rilevamento* – paragrafo 4, *Risposta* – paragrafo 5, *Recupero* – paragrafo 6); che all'interno di queste "macro-aree" (*funzioni* o fasi di rilevazione) sono poi definite le *categorie* di misure di sicurezza [identificate con una sotto-numerazione (2.1, 2.2, 2.3, *etc.*), quali, ad esempio, *Gestione degli asset* (*Asset Management*) (*ID.AM*), *Governance* (*ID.GV*), *Valutazione del rischio* (*Risk Assessment*) (*ID.RA*), *Strategia della gestione del rischio* (*ID.RM*), *etc.*; che, infine, ciascuna categoria si articola al suo interno in sottocategorie (ad esempio, 2.1.1 ID.AM-1, 2.1.2 ID.AM-2, 2.1.3 ID.AM-3, *etc.*), ulteriormente suddivise in specifiche azioni.

7.3. Nel secondo periodo del comma 1 l'articolo 7 informa inoltre che *'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*". Non è questa la sede per entrare nel merito delle scelte redazionali e di strutturazione logica dell'allegato compiute dall'Amministrazione (evidentemente dettate dall'esigenza di riprendere le classificazioni usate nel *Framework* nazionale per la *cybersecurity* e la *data protection*", edizione 2019, o altro riferimento tecnico), ma è doveroso rilevare come la costruzione prescelta appaia inutilmente complicata, lì dove sarebbe stato più semplice e chiaro usare la tabella di corrispondenza come indice e radice logica all'interno della quale organizzare l'elencazione, la classificazione e la descrizione delle diverse misure di sicurezza per "*ambiti*" (come definiti dalla legge) e categorie e sottocategorie riferite a ciascuna funzione. Nella relazione illustrativa si chiarisce, circa il rapporto di corrispondenza tra le misure di sicurezza individuate dal presente decreto e i nove ambiti delineati dall'articolo 1, comma 3, lettera *b*), del decreto-legge, che "*In ragione della richiamata scelta operata nei sensi di assumere, quale base di riferimento, il Framework nazionale, e delle conseguenti ricadute redazionali e sistematiche sull'elaborazione del testo regolamentare comprensivo degli allegati, l'allegato B è corredato (in appendice n. 1) di una tabella di corrispondenza tra gli ambiti del decreto-legge e le misure individuate per ciascuno di tali ambiti. Nel*

caso in cui una misura attenga a più ambiti, la stessa è stata riportata in corrispondenza di ciascuno di essi. Nel caso in cui, infine, in relazione ad uno specifico ambito trovi applicazione soltanto una parte specifica di una determinata misura, anche tale limitazione è stata opportunamente evidenziata". È dunque evidente alla stessa Amministrazione proponente la macchinosità del sistema prescelto, evidentemente imposto dalla maggiore interoperabilità e utilità pratica del modello costituito dal "*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 Laboratorio nazionale di *Cybersecurity* 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). Deve tuttavia evidenziarsi – lasciando ogni valutazione in merito all'Amministrazione - come la "combinazione" tra gli "*ambiti*" definiti dal legislatore e la ripartizione articolata in "*funzioni*" nell'allegato B lasci spazio a dubbi sulla reale corrispondenza tra queste due classificazioni e ponga obiettive difficoltà di lettura.

7.4. Sempre ai fini di una più agevole leggibilità del testo, sarebbe utile aggiungere nell'articolo 7, stante questa sua funzione esplicativa di descrizione dei contenuti dell'allegato B, una specificazione relativa all'appendice 2 contenuta nell'allegato B ora detto, appendice la cui funzione e il cui significato si ricavano solo indirettamente dal testo del successivo articolo 8. L'appendice n. 2 dell'allegato B reca, peraltro, la sintetica e poco significativa rubrica "*Categorie*", che non ne consente un'immediata comprensione (denominazione che, peraltro, rischia di ingenerare anche equivoci, rispetto alle "*categorie*" di incidenti definite nell'allegato A e rispetto alle "*categorie*" tipologiche di classificazione delle misure di sicurezza previste nell'allegato B). Sarebbe utile integrare tale rubrica con la specificazione, ricavabile dall'articolo 8, che le "*categorie*" "A" e "B" di cui

all'appendice 2 servono alla ripartizione delle misure di sicurezza agli effetti dei termini di adozione e di comunicazione dell'avvenuta adozione da parte dei soggetti inclusi nel perimetro. Potrebbe a tali fini riprendersi l'indicazione contenuta nella relazione illustrativa, nella quale le due macro-categorie in cui sono state suddivise le misure individuate nell'allegato B includono – nella "categoria" A – quelle da adottare entro 6 mesi e – nella "categoria" B – quelle da adottare entro 24 mesi.

8. Articolo 8 (*Modalità e termini di adozione delle misure di sicurezza*).

8.1. Il comma 1 prevede un unico termine per l'adozione e per la comunicazione dell'avvenuta adozione delle misure di sicurezza; sarebbe più logico prevedere o due termini diversi, o il solo termine di comunicazione dell'avvenuta adozione. Non risulta inoltre indicata l'Autorità alla quale la comunicazione deve essere destinata (il CSIRT italiano o il DIS; sembra il DIS, da quanto si può evincere dal comma 4). Sotto il profilo della tecnica redazionale del testo, conviene distinguere – come indicato anche per l'analoga previsione dell'articolo 3, comma 3 (cfr. sopra, paragrafo 3.2) - in due distinte statuizioni i due comandi giuridici contenuti nella disposizione (l'adozione e comunicazione dell'adozione delle misure di sicurezza e le modalità di comunicazione). Sarebbe dunque preferibile scindere in due commi (o in due diversi periodi) la disposizione in esame, nei seguenti termini: "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) . . . b) . . ., etc.* 2. *I soggetti di cui al comma 1, immediatamente dopo l'avvenuta adozione delle misure di sicurezza di cui all'allegato B, ne danno comunicazione [al CSIRT italiano o 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, con il modello reso disponibile dal DIS 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*".

8.2. Nella lettera *a*) del comma 1 è previsto che "*qualora la trasmissione avvenga*

in una data antecedente a quella di entrata in vigore del presente regolamento, [la comunicazione deve essere effettuata] *entro sei mesi da quest'ultima data*". Tale formulazione non è corretta, poiché qualunque data anteriore all'entrata in vigore del regolamento non può che essere, per definizione, passata e deve quindi essere indicata con il tempo passato del congiuntivo: "*sia avvenuta*" (e non "*avvenga*").

8.3. L'ultimo periodo della lettera *a*) deve essere riformulato come segue: "*I soggetti inclusi nel perimetro che abbiano già adottato le misure di sicurezza di cui alla categoria B dell'appendice n. 2 dell'allegato B, ne danno comunicazione indicando altresì le modalità di adozione*".

8.4. Per la lettera *b*) valgono le stesse considerazioni ora svolte per la lettera *a*). Inoltre, la parola "*quelle*", al primo rigo, va sostituita con le parole "*le misure di sicurezza*".

9. Articolo 9. (*Tutela delle informazioni*).

9.1. La norma riguarda le misure minime di sicurezza in tema di protezione fisica e logica dei dati e di integrità delle reti e dei sistemi informativi, ossia delle misure di sicurezza relative agli "*ambiti*" individuati dai numeri 3) e 4) della lettera *b*) del comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019. Ora, mentre tali "macro-aree" di intervento delle misure di sicurezza – elencate nei nove numeri in cui si articola la citata lettera *b*) – sono definite "*ambiti*" nell'ultimo *Considerato* del preambolo del presente schema di decreto, nella relazione illustrativa e nell'articolo 7, comma 1 - nell'articolo 9 in esame, invece, si parla (ancora una volta) di "*categorie*" ("*di cui all'articolo 1, comma 3, lettera b), numeri 3 e 4, del decreto-legge*"). Come già segnalato sopra, nel paragrafo 7.4 a proposito dell'articolo 7, vi è un uso eccessivo e promiscuo, nel testo regolamentare in esame, del termine "*categoria*", che risulta riferito a oggetti e concetti diversi (vi sono già le "*categorie*" di incidenti definite nell'allegato A, le "*categorie*" tipologiche di classificazione delle misure di sicurezza previste nell'allegato B e le "*categorie*" A e B dell'appendice n. 2, che servono a distinguere le misure di sicurezza in base al

termine di adozione e comunicazione). Sarebbe pertanto preferibile usare, in luogo del termine "*categorie*", il termine "*ambiti*" o "*macro-aree*", con riferimento all'elenco suddetto della lettera *b*) del comma 3 della norma primaria.

10. Articolo 10 (*Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*).

Nessuna osservazione

11. Articolo 11 (*Disposizioni finali*).

Nessuna osservazione.

P.Q.M.

Nei sensi suesposti è il parere della Sezione.

L'ESTENSORE
Paolo Carpentieri

IL PRESIDENTE
Paolo Troiano

IL SEGRETARIO
Campobasso Maurizia