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

Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. (21G00089)

(GU n.138 del 11-6-2021)

Vigente al: 26-6-2021

Capo I
Disposizioni generali

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica e, in particolare, l'articolo 1, comma 3;

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

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

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

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

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

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

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

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

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

Visto il decreto del Presidente del Consiglio dei ministri 8 agosto 2019, recante disposizioni sull'organizzazione e il funzionamento del

Computer security incident response team - CSIRT italiano, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 262 dell'8 novembre 2019;

Visto il «Framework nazionale per la cybersecurity e la data protection», edizione 2019 (Framework nazionale), realizzato dal Centro di ricerca di cyber intelligence and information security (CIS) dell'Universita' Sapienza di Roma e dal Cybersecurity national lab del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorita' 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, nonche' per il loro continuo monitoraggio;

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

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

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

Sulla proposta del Comitato interministeriale per la sicurezza della Repubblica;

Adotta
il seguente regolamento:

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 piu' 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 operativita' del bene ICT, ovvero compromissione della disponibilita', integrita', o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali;

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

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

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

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

Capo II
Notifiche di incidente

Art. 2

Tassonomia degli incidenti

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

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

Art. 3

Notifica degli incidenti aventi impatto su beni ICT

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

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

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

4. I soggetti inclusi nel perimetro effettuano la notifica di cui ai commi 1, 2 e 3 entro sei ore, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A, ed entro un'ora, qualora

si tratti di un incidente individuato nella tabella 2 del medesimo allegato. I predetti termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza, a seguito delle evidenze ottenute, anche mediante le attivita' di monitoraggio, test e controllo di cui all'articolo 1, comma 3, lettera b), numero 6, del decreto-legge, effettuate sulla base delle misure di sicurezza di cui all'allegato B, di un incidente riconducibile a una delle tipologie individuate nell'allegato A. La notifica e' 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 modalita' definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

5. Qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi, tra cui le specifiche vulnerabilita' 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 e' integrata tempestivamente dal momento in cui il soggetto incluso nel perimetro ne e' venuto a conoscenza, salvo che l'autorita' giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

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

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

8. Una volta definiti e avviati i piani di attuazione delle attivita' per il ripristino dei beni ICT impattati dall'incidente oggetto di notifica, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi dei commi 1, 2 e 3, tramite i canali di comunicazione di cui al comma 4, ne da' tempestiva comunicazione al CSIRT italiano e trasmette, altresi', 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'autorita' giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

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

10. Sino al 31 dicembre 2021, restano fermi per i soggetti inclusi nel perimetro, che effettuano, ai sensi del comma 2, le notifiche in via sperimentale, gli obblighi di notifica di cui agli articoli 12,

comma 5, e 14, comma 4, del decreto legislativo n. 65 del 2018, nonche' quelli previsti ai sensi dell'articolo 16-ter del decreto legislativo n. 259 del 2003 e delle correlate disposizioni attuative.

Art. 4

Notifica volontaria degli incidenti

1. Al di fuori dei casi di cui all'articolo 3, i soggetti inclusi nel perimetro possono notificare, su base volontaria, gli incidenti, relativi ai beni ICT, non indicati nelle tabelle di cui all'allegato A, ovvero gli incidenti, indicati nelle tabelle di cui all'allegato A, relativi a reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai beni ICT. La notifica e' 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 modalita' definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano.

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

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

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

Art. 5

Trasmissione delle notifiche

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

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

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

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

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

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

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

Art. 6

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

1. In materia di notifica degli incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione

delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

Capo III
Misure di sicurezza

Art. 7

Misure di sicurezza

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

Art. 8

Modalita' e termini di adozione delle misure di sicurezza

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

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

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

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

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

4. Qualora un soggetto incluso nel perimetro proceda, ai sensi degli articoli 7 e 9 del regolamento adottato con il DPCM n. 131 del 2020, all'aggiornamento dell'elenco dei beni ICT, valuta contestualmente se e' 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 modalita', con il modello di cui al comma 1, nei seguenti termini:

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

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

5. In ogni altro caso in cui un soggetto incluso nel perimetro abbia proceduto ad adeguare le misure di sicurezza adottate ai sensi

del presente articolo, ne comunica, entro sei mesi, le relative modalita' con il modello di cui al comma 1.

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

Art. 9

Tutela delle informazioni

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

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

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

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

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

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

3. Resta ferma l'adozione, da parte dei soggetti inclusi nel perimetro, delle misure di sicurezza di livello piu' 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 sara' inserito nella raccolta ufficiale degli atti normativi della Repubblica

italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 14 aprile 2021

Il Presidente: Draghi

Visto, il Guardasigilli: Cartabia

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

Allegato A
(articolo 2)

Tassonomia degli incidenti

Identificativo (incidente con impatto-ICP)	Categoria	Descrizione
ICP-A-1	Infezione (Initial exploitation)	Infezione (Initial exploitation). Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o malware veicolato attraverso vettori di infezione o sfruttando vulnerabilita' 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 indisponibilita', di perdita irreversibile o di corruzione irreversibile dei dati provenienti dalle componenti di campo (attuatori e sensori).
ICP-A-5		Dati hot-replica e/o cold-replica e/o sito(i) di disaster recovery e/o backup, se previsti, persi o corrotti in modo irreversibile.
ICP-A-6		Perdita di confidenzialita' o integrita'.
ICP-A-7		Perdita e/o corruzione dati irreversibile.

ICP-A-8		Perdita e/o compromissione di chiavi di cifratura e/o certificati.
ICP-A-9		Perdita e/o compromissione di credenziali utenti.
ICP-A-10		Violazione del livello di servizio atteso, definito dal soggetto incluso nel perimetro ai sensi di quanto previsto dalle misure di sicurezza di cui all'allegato B, in termini di impossibilita' di accesso fisico alle componenti.
ICP-A-11	Installazione	Ottenimento di privilegi di livello superiore (Privilege Escalation). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere
	(Establish persistence)	permessi di livello superiore.
ICP-A-12		Persistenza (Persistence). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere persistenza di codice malevolo o d'accesso.
ICP-A-13		Evasione delle difese (Defence Evasion). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche attraverso cui sono stati effettivamente elusi i sistemi di sicurezza.
ICP-A-14		Comando e Controllo (Command and Control). Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.
ICP-A-15		Esplorazione (Discovery). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attivita' di ricognizione.
ICP-A-16	Movimenti laterali (Lateral Movement)	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		Raccolta (Collection). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad raccogliere, dall'interno della rete, dati di

	Azioni sugli obiettivi (Action on objs)	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		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	Azioni sugli obiettivi (Actions on objectives)	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 disponibilita', 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
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.

2.2 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.

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

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

2.5 Gestione del rischio relativo alla catena di approvvigionamento (ID.SC): Le priorita', 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.

3. PROTEZIONE (PROTECT)

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

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

3.3 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'integrita', la confidenzialita' e la disponibilita' delle informazioni.

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 responsabilita', impegno da parte del management e coordinamento tra le diverse entita' organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset.

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

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. 17

4. RILEVAMENTO (DETECT)

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

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. ...

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

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.

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

5.3 Analisi (RS.AN): Vengono condotte analisi per assicurare

un'efficace riposta e supporto alle attivita' di ripristino.

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.

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.

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

6.3 Comunicazione (RC.CO): Le attivita' 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).

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

APPENDICE n. 2 - CATEGORIE

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, altresi', indicate raccomandazioni, la cui attuazione e' demandata alle valutazioni di ciascun soggetto incluso nel perimetro.

2. Per ogni misura e' fornita una specifica piu' dettagliata dell'implementazione minima attesa, nonche' delle modalita' 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, e' 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 e' stato mantenuto il termine cybersecurity che, nell'ambito del presente allegato, e' 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 modalita' 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 cosi' come indicati nel modello dei beni ICT.

2. Tutti sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete e' 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 cosi' come indicati nel modello dei beni ICT.

2. L'installazione delle piattaforme e delle applicazioni software e' consentito esclusivamente per quelle approvate.

3. Si raccomanda, ove possibile e in relazione alla criticita' 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, nonche' 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 cosi' come indicati nell'modello dei beni ICT.

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

1. E' definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilita', per tutto il personale e per eventuali terze parti.

2. All'interno dell'organizzazione di cui al punto 1 e' istituita e resa nota alle articolazioni competenti del soggetto l'articolazione per l'implementazione del perimetro.

3. E' 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 professionalita' 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 attivita' connesse all'articolo 5 del decreto-legge e alle attivita' di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica (NSC), e con i soggetti incaricati dello svolgimento delle attivita' 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 responsabilita'. L'elenco e' 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 e' 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: E' 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 e' compilato e trasmesso secondo le modalita' 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'operativita' dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.

2.3.1 ID.RA-1: Le vulnerabilita' 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 attivita' 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 periodicita' e le modalita' di esecuzione e, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT cosi' 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 vulnerabilita' rilevate e il relativo livello di impatto sulla sicurezza;

c. il livello di esposizione delle risorse del sistema cui e' possibile accedere a seguito dello sfruttamento delle vulnerabilita'.

2.3.2 ID.RA-5: Le minacce, le vulnerabilita', le relative probabilita' 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 vulnerabilita', delle relative probabilita' 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 probabilita' di accadimento;

b. qualora disponibili, le vulnerabilita' emerse a seguito dell'esecuzione del piano di cui alla sottocategoria ID.RA-1 e a seguito dell'adozione delle misure di cui alla sottocategoria DE.CM-8;

c. i potenziali impatti ritenuti significativi sui beni ICT, opportunamente descritti e valutati;

d. l'identificazione, l'analisi e la ponderazione del rischio.

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

1. Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorita'.

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, e' approvato da parte dei vertici del soggetto.

2.4 Strategia della gestione del rischio (ID.RM): Le priorita' 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 e' 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 priorita', 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), nonche' 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, gia' a partire dalla fase di progettazione;

b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilita', con la possibilita' 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'affidabilita' tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno:

1) della qualita' 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 priorita' data agli aspetti di sicurezza;

2) della capacita' 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), nonche' 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, cosi' come indicati nel modello dei beni ICT.

3. Si raccomanda, ove possibile e in relazione alla criticita' 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'affidabilita' tecnica di cui al punto 1, lettera d, anche tenendo conto:

1) della disponibilita' del fornitore a condividere il codice sorgente;

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

3) dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticita' e l'integrita' 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 qualita' 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 modalita' 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, nonche' un registro di quelli effettuati e la relativa documentazione.

3. PROTEZIONE (PROTECT)

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

alle transazioni autorizzate

3.1.1 PR.AC-1: Le identita' 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 identita' 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 e' 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 e' 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 e' proporzionale al rischio.

3. Esiste un documento aggiornato di dettaglio contenente almeno:

a. le politiche di sicurezza adottate per la definizione delle attivita' 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 e' possibile accedere da remoto e con quali modalita';

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 e' 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'integrita' di rete e' 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 modalita' con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.

3.1.6 PR.AC-7: Le modalita' 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 modalita' 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 modalita' 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 responsabilita'

1. Esiste un documento aggiornato di dettaglio, che indica i contenuti dell'istruzione fornita agli utenti con privilegi e le modalita' 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'integrita', la confidenzialita' e la disponibilita' delle informazioni.

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

1. I dati digitali trattati mediante l'impiego di beni ICT, ivi compresi quelli relativi alla descrizione degli stessi beni, la cui compromissione sotto il profilo della disponibilita', integrita' e riservatezza puo' avere impatto sullo svolgimento delle funzioni o dei servizi essenziali per i quali il soggetto e' stato incluso nel perimetro, sono conservati, elaborati, ovvero estratti esclusivamente mediante l'impiego di infrastrutture fisiche e tecnologiche, anche se esternalizzate (ad esempio tramite cloud computing), localizzate sul territorio nazionale. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity.

2. I dati digitali utilizzati dalle infrastrutture deputate alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), nonche' le infrastrutture di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), devono essere localizzati sul territorio nazionale, salvo motivate e documentate ragioni di natura normativa o tecnica. In presenza di tali motivazioni i predetti dati e infrastrutture non devono comunque essere localizzati al di fuori del territorio dell'Unione europea.

3. Qualora opportunamente cifrati, i dati digitali di backup, anche se esternalizzati (ad esempio tramite cloud computing), possono essere conservati al di fuori del territorio nazionale, ma non al di fuori del territorio dell'Unione europea e le chiavi di cifratura devono essere comunque custodite all'interno del territorio nazionale. Le operazioni di cifratura e decifratura devono comunque essere eseguite mediante infrastrutture localizzate sul territorio nazionale.

4. Per i dati digitali e le infrastrutture di cui ai punti 2 e 3, ove localizzati al di fuori del territorio nazionale, l'applicazione delle misure ID.RA-5 e ID.RA-6 deve tenere opportunamente conto della localizzazione estera.

5. Le disposizioni di cui al punto 1, 2, 3 e 4 non si applicano alle sedi diplomatiche o consolari.

6. Esiste un documento aggiornato che descrive in quali sedi e infrastrutture sono conservati, elaborati ovvero estratti i dati digitali relativi ai beni ICT di cui ai punti 1, 2 e 3, ovvero le fattispecie di cui al punto 4.

7. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:

a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;

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

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

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:

a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati;

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

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

1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:

a. le politiche di sicurezza adottate per l'accesso ai dati;

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

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

b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi e' 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 e' 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 responsabilita', impegno da parte del management e coordinamento tra le diverse entita' 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 funzionalita')

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 nonche' dal sito(i) di disaster recovery, anche al fine di caratterizzare gli incidenti di cui all'articolo 1, comma 3, lettera a) del decretolegge.

2. Esiste un documento aggiornato di dettaglio contenente i piani di continuita' operativa/disaster recovery, nonche' quelli di risposta e di recupero in caso di incidenti, che comprende almeno:

a. le politiche e i processi impiegati per identificare le priorita' degli eventi;

b. le fasi di attuazione dei piani;

c. i ruoli e le responsabilita' 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 attivita' di istruzione, formazione ed esercitazione svolte.

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

1. Esiste un documento aggiornato di dettaglio che indica almeno:

a. le politiche di sicurezza adottate per gestire le vulnerabilita';

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 e' 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 e' 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 tempestivita' relative alla sicurezza, dovra' essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo e il relativo codice oggetto dovra' essere custodito per almeno 24 mesi.

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

1. La manutenzione delle risorse e dei sistemi (ivi incluse le attivita' relative alle funzioni di sicurezza) svolta da remoto e' 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 funzionalita' amministrative disponibili.

5. Tutti i log relativi alle sessioni di comunicazione remota e alle attivita' 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 e' 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'integrita' e alla disponibilita' 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 connettivita', nonche' applicative;

b. esiste un sito di disaster recovery.

2. Esistono meccanismi per garantire la continuita' 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 attivita' 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 piu' 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 attivita' di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, e' 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 attivita' dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonche' 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 vulnerabilita'

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 criticita' 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 responsabilita' 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 responsabilita' per le attivita' 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 responsabilita' 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, nonche' 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 attivita' 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 responsabilita' 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 responsabilita' di cui ai punti 1 e 2;

b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilita' di cui ai punti 1 e 2;

c. le modalita' 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 attivita' di ripristino.

5.3.1 RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilita' 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'Autorita' di riferimento del proprio settore produttivo, nonche' di eventuali CERT e Information Sharing & Analysis Centre (ISAAC) di riferimento sono monitorati.

3. Esiste un documento aggiornato che descrive, almeno:

a. le modalita' per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attivita' di cui ai punti 1 e 2;

b. i processi, i ruoli, le responsabilita' e gli strumenti tecnici per lo svolgimento delle attivita' 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 vulnerabilita' sono mitigate o documentate come rischio accettato

1. Le vulnerabilita' sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilita' (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 attivita' future.

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

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

6.3 Comunicazione (RC.CO): Le attivita' 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 attivita' 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 attivita' 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) integrita' 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 continuita' del servizio	
	3.4.4 PR.IP-9
	3.6.3 PR.PT-5
	6.1.1 RC.RP-1
	6.2.1 RC.IM-2
6) monitoraggio, test e controllo	2.3.1 ID.RA-1
	2.5.4 ID.SC-4
	3.1.1 PR.AC-1, limitatamente al punto

	3
	3.1.3 PR.AC-3, limitatamente al punto 1
	3.5.1 PR.MA-1, limitatamente al punto 3
	3.6.2 PR.PT-4
	4.1.1 DE.AE-3
	4.2.1 DE.CM-1
	4.2.2 DE.CM-4
	4.2.3 DE.CM-7
	4.2.4 DE.CM-8
	4.3.1 DE.DP-1
7) formazione e consapevolezza	3.2.1 PR.AT-1
	3.2.2 PR.AT-2
	3.4.4 PR.IP-9, limitatamente ai punti 3 e 4
	5.2.1 RS.CO-1, limitatamente ai punti 3, 4 e 5
8) affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti	2.1.4 ID.AM-6, limitatamente al punto 8
	2.5.1 ID.SC-1
	2.5.2 ID.SC-2
	2.5.3 ID.SC-3
	2.5.4 ID.SC-4

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

Misure del presente allegato	Categorie di cui all'art. 8
2.1.1 ID.AM-1	A
2.1.2 ID.AM-2	B
2.1.3 ID.AM-3	A
2.1.4 ID.AM-6	A

2.2.1 ID.GV-1	A
2.2.2 ID.GV-4	A
2.3.1 ID.RA-1	A
2.3.2 ID.RA-5	A
2.3.3 ID.RA-6	B
2.4.1 ID.RM-2	A
2.5.1 ID.SC-1	A
2.5.2 ID.SC-2	B
2.5.3 ID.SC-3	B
2.5.4 ID.SC-4	A
3.1.1 PR.AC-1	B
3.1.2 PR.AC-2	B
3.1.3 PR.AC-3	B
3.1.4 PR.AC-4	B
3.1.5 PR.AC-5	B
3.1.6 PR.AC-7	B
3.2.1 PR.AT-1	A
3.2.2 PR.AT-2	A
3.3.1 PR.DS-1	B
3.3.2 PR.DS-3	A
3.3.3 PR.DS-5	B
3.3.4 PR.DS-6	B
3.3.5 PR.DS-7	B
3.4.1 PR.IP-1	B
3.4.2 PR.IP-3	B
3.4.3 PR.IP-4	B
3.4.4 PR.IP-9	A
3.4.5 PR.IP-12	A
3.5.1 PR.MA-1	B
3.5.2 PR.MA-2	B
3.6.1 PR.PT-1	B
3.6.2 PR.PT-4	B
3.6.3 PR.PT-5	B
4.1.1 DE.AE-3	B

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

Allegato C
(articolo 9)

Misure minime di sicurezza per la tutela delle informazioni

1. Trattamenti con l'ausilio di strumenti elettronici

a) Identificazione degli utenti e gestione delle identita' 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 disponibilita' dei dati e dei sistemi;

l) adozione di tecniche di cifratura.

2. Misure di sicurezza fisica e documentale

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

b) deve essere individuata la figura di un responsabile incaricato della gestione delle informazioni, preferibilmente gia' 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 necessita' di conoscere (need to know) e deve essere tracciata su apposito registro;

f) la riproduzione dei documenti puo' 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.