REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, AI SENSI DELL'ARTICOLO 33-SEPTIES, COMMA 4, DEL DECRETO-LEGGE 18 OTTOBRE 2012, N. 179, CONVERTITO, CON MODIFICAZIONI, DALLA LEGGE 17 DICEMBRE 2012, N. 221

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE
IL DIRETTORE GENERALE

VISTA la legge 23 agosto 1988, n. 400, recante: «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri»;

VISTO il 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);

VISTO il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;

VISTO 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 cibersicurezza e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»);

VISTA la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

VISTA la legge 21 giugno 1986, n. 317, recante: «Disposizioni di attuazione di disciplina europea in materia di normazione europea e procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione»;

VISTO il decreto legislativo 30 marzo 2001, n. 165, recante: «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche», e, in particolare, l'articolo 1, comma 2;

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante: «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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»;

VISTO il decreto legislativo 7 marzo 2005, n. 82, recante: «Codice dell'amministrazione digitale»;

VISTA la legge 31 dicembre 2009, n. 196, recante «Legge di contabilità e finanza pubblica»;

VISTO il decreto legislativo 18 maggio 2018, n. 65, recante: «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 decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, recante: «Ulteriori misure urgenti per la crescita del Paese», e, in particolare, l'articolo 33-*septies* che prevede il consolidamento e la razionalizzazione dei siti e delle infrastrutture digitali del Paese demandando all'Agenzia per la cybersicurezza nazionale, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri e nel rispetto della disciplina introdotta dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, l'adozione di un regolamento per stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione nonché le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione e, infine, i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni previste ai commi 1 e 1-*bis* dello stesso articolo 33-*septies* e le modalità del procedimento di qualificazione dei servizi cloud per la pubblica amministrazione;

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»;

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale», e, in particolare, l'articolo 7, comma 1, lettere *m*) e *m-ter*), che attribuisce all'Agenzia per la cybersicurezza nazionale tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge n. 179 del 2012, e la qualificazione dei servizi *cloud* per la pubblica amministrazione, nonché l'articolo 17, comma 6, secondo periodo;

VISTO il decreto-legge 8 ottobre 2021, n.139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205, recante: «Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali», e, in particolare, l'articolo 9, comma 1, lettere a) e i), e comma 7;

VISTO il decreto del Presidente del Consiglio dei ministri del 9 dicembre 2021, n. 223, recante: «Regolamento di organizzazione e di funzionamento dell'Agenzia per la cybersicurezza nazionale»;

VISTO il decreto del Presidente del Consiglio dei ministri del 17 maggio 2022, con cui, ai sensi dell'articolo 7, comma 1, lettera b), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è stata adottata la "Strategia nazionale di cybersicurezza 2022-2026" comprensiva del relativo "Piano di implementazione 2022- 2026", cui è stata data comunicazione nella Gazzetta Ufficiale della Repubblica italiana del 1° giugno 2022, n. 127;

VISTO il decreto del Presidente del Consiglio dei ministri del 1° settembre 2022, recante: «Modalità e termini per assicurare il trasferimento delle funzioni, dei beni strumentali e della documentazione dall'Agenzia per l'Italia digitale e dal Dipartimento per la trasformazione digitale all'Agenzia per la cybersicurezza nazionale», pubblicato nella *Gazzetta Ufficiale* delle Repubblica italiana del 20 ottobre 2022, n. 246;

VISTO il decreto del Presidente del Consiglio dei ministri del 1° settembre 2022, n. 166, recante: «Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico»*;*

VISTO il decreto del Presidente del Consiglio dei ministri del 10 marzo 2023, con il quale è stato conferito al Prefetto Bruno Frattasi l'incarico di Direttore generale dell'Agenzia per la cybersicurezza nazionale;

VISTA la determinazione del 15 dicembre 2021, n. 628, dell'Agenzia per l'Italia digitale, di adozione del «Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione», di cui è stato dato avviso nella Gazzetta Ufficiale delle Repubblica italiana n. 19 del 25 gennaio 2022 (c.d. regolamento "Cloud della PA");

VISTA la determina del 18 gennaio 2022, n. 306, dell'Agenzia per la cybersicurezza nazionale, recante l'adozione del modello per la predisposizione dell'elenco e della classificazione di dati e di servizi;

VISTA la determina del 18 gennaio 2022, n. 307, dell'Agenzia per la cybersicurezza nazionale, di adozione dell'Aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché requisiti di qualificazione dei servizi cloud per la pubblica amministrazione;

VISTO il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 2 gennaio 2023, protocollo n. 29, recante: «Nuovo processo di qualificazione dei servizi cloud per la pubblica amministrazione», con cui è stata data comunicazione nella Gazzetta Ufficiale della Repubblica italiana del 10 gennaio 2023, n. 7;

VISTO il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale dell'8 febbraio 2023, prot. n. 5489, recante: «Differimento dei termini per l'adeguamento delle infrastrutture per la pubblica amministrazione», con cui è stata data comunicazione nella Gazzetta Ufficiale della Repubblica italiana del 9 marzo 2023, n. 58;

VISTO il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 28 luglio 2023, prot. n. 20610, recante: «Modifiche ai livelli minimi delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni», con cui è stata data comunicazione nella Gazzetta Ufficiale della Repubblica italiana del 16 agosto 2023, n.190;

VISTA la circolare dell'Agenzia per l'Italia Digitale del 14 giugno 2019, n. 1, recante: «Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali»;

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) della Presidenza del Consiglio dei ministri, 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;

TENUTO conto della Strategia Cloud Italia che detta gli indirizzi strategici per il percorso di migrazione verso il cloud dei dati e dei servizi digitali della pubblica amministrazione, e illustra i criteri di classificazione dei dati e dei servizi e la composizione della infrastruttura ad alta affidabilità;

CONSIDERATO il parere reso all'Agenzia per l'Italia digitale dal Garante per la protezione dei dati personali il 16 dicembre 2021, in merito allo schema di regolamento in materia di servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-*septies*, del decreto-legge 18 ottobre 2012, n. 179;

ESPERITA la procedura di informazione ai sensi della Direttiva (UE) n. 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015, con comunicazione del 1 febbraio 2024;

ACQUISITO il parere del Garante per la protezione dei dati personali, reso nell'adunanza del 9 maggio 2024;

D'INTESA con il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri;

Adotta il seguente Regolamento

Capo I
Disposizioni di carattere generale

Articolo 1
(Definizioni)

1. Ai fini del presente Regolamento si intende per:
   a) «ACN», l'Agenzia per la cybersicurezza nazionale, di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;
   b) «AgID», l'Agenzia per l'Italia digitale, di cui all'articolo 19, del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;
   c) «amministrazioni centrali», le amministrazioni centrali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
   d) «amministrazioni locali», le amministrazioni locali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
   e) «amministrazioni», le amministrazioni centrali di cui alla lettera c) e le amministrazioni locali di cui alla lettera d);
   f) «catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni», il catalogo a cura dell'ACN, reso disponibile tramite la piattaforma digitale, in cui è pubblicato l'elenco delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e dei servizi cloud per le pubbliche amministrazioni, corredati dalle relative informazioni descrittive;
   g) «cloud computing», paradigma che abilita l'accesso via rete ad un insieme condivisibile,

scalabile ed elastico di risorse fisiche o virtuali attivabile autonomamente su richiesta dall'utente;

h) «dati dell'amministrazione», le informazioni trattate dall'amministrazione, o da terzi per conto dell'amministrazione;
i) «dati digitali dell'amministrazione», i dati dell'amministrazione trattati tramite reti e sistemi informativi dell'amministrazione o di terzi per conto dell'amministrazione;
j) «servizi dell'amministrazione», servizi erogati verso terzi o internamente all'amministrazione;
k) «servizi digitali», servizi informatici erogati tramite reti e sistemi informativi dell'amministrazione o tramite reti e sistemi informativi di terzi per conto dell'amministrazione, verso terzi, internamente all'amministrazione o a supporto di servizi dell'amministrazione, ad esclusione dei servizi ICT di base;
l) «servizi ICT di base», servizi informatici erogati tramite reti e sistemi informativi a supporto di servizi digitali dell'amministrazione, quali i servizi infrastrutturali ICT, i servizi di sicurezza ICT e la connettività;
m) «Infrastrutture digitali per le pubbliche amministrazioni», le infrastrutture digitali tramite le quali sono erogati i servizi digitali delle amministrazioni, ivi inclusi:
    1. i Centri di Elaborazione Dati (CED), ovvero, ai sensi dall'articolo 33-septies, comma 2, del decreto-legge n. 179 del 2012, i siti che ospitano reti e sistemi informativi atti alla erogazione di servizi interni alle amministrazioni e servizi erogati esternamente dalle amministrazioni che al minimo comprende risorse di calcolo, apparati di rete per la connessione e sistemi di memorizzazione di massa;
    2. l'infrastruttura promossa dalla Presidenza del Consiglio dei ministri di cui all'articolo 33-*septies*, comma 1, del decreto-legge n. 179 del 2012;
    3. i componenti di un'infrastruttura digitale messi a disposizione da terze parti e finalizzati all'erogazione di servizi cloud per la pubblica amministrazione e di cui possono avvalersi anche le infrastrutture digitali di cui al punto 1 (c.d. *housing*);
    4. i componenti di un'infrastruttura digitale, eventualmente messi a disposizione da terze parti, finalizzati all'incremento delle prestazioni nell'erogazione in prossimità dei servizi digitali delle amministrazioni (c.d. infrastrutture di prossimità). Nello specifico, si può trattare di un singolo server o di un altro insieme di risorse di calcolo connesse, operati nell'ambito di un'infrastruttura di prossimità, generalmente situati all'interno di un data center che opera all'estremità dell'infrastruttura, e quindi fisicamente più vicini agli utenti destinatari rispetto a un nodo cloud in un data center centralizzato;
n) «Infrastrutture dei servizi cloud per le pubbliche amministrazioni», le infrastrutture digitali di cui alla lettera m), fornite da un operatore di infrastrutture digitali, tramite le quali sono erogati i servizi cloud per le pubbliche amministrazioni;
o) «operatore di infrastrutture digitali», soggetto, pubblico o privato, che, nel rispetto dei limiti fissati dal presente Regolamento, opera un'infrastruttura digitale per le pubbliche amministrazioni ovvero finalizzata all'erogazione di servizi cloud per le pubbliche amministrazioni;
p) «servizi cloud», servizi informatici e risorse computazionali erogati mediante il paradigma cloud computing su richiesta dell'utente tramite internet da un fornitore di servizi cloud, differenziati, sulla base del modello computazionale offerto, in tre categorie di servizi:
    1) «sistemistici infrastrutturali, c.d. Infrastructure-as-a-Service (IaaS)», per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
    2) «piattaforme computazionali, c.d. Platform-as-a-Service (PaaS)», per l'erogazione di ambienti, pre-configurati e amministrati per lo sviluppo di specifiche applicazioni, ad esempio per lo sviluppo software, la gestione di dati o di applicazioni;
    3) «applicativi, c.d. Software-as-a-Service (SaaS)», per l'erogazione di un'applicazione agli utenti finali, ad esempio la posta elettronica o altri sistemi di collaborazione remota. Tra i

modelli di servizio offerti dalle piattaforme di Cloud computing, il Software as a Service (SaaS) identifica una classe di servizi fully-managed in cui il gestore del servizio, ovvero il fornitore di servizi cloud, si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura digitale propria o di terzi), lasciando al fruitore del servizio, ovvero le pubbliche amministrazioni, il solo ruolo di utilizzatore delle funzionalità offerte.

q) «servizi cloud per le pubbliche amministrazioni», servizi cloud tramite i quali sono erogati servizi digitali delle amministrazioni;
r) «compromissione», la compromissione di dati o servizi digitali in termini di confidenzialità, integrità o disponibilità;
s) «qualificazione dei servizi cloud», processo di verifica per garantire che i servizi cloud per le pubbliche amministrazioni siano in possesso delle caratteristiche necessarie per trattare dati e servizi in funzione della loro classificazione, assicurando, in particolare, opportuni livelli di qualità, di performance, di scalabilità, di portabilità, nonché di sicurezza;
t) «adeguamento», l'attività propedeutica alla trasmissione all'ACN, da parte di un operatore di infrastrutture digitali ovvero di un fornitore di servizi cloud pubblico, di una relazione di conformità delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni ovvero dei servizi cloud per la pubblica amministrazione ai requisiti fissati dal presente Regolamento;
u) «piattaforma digitale», la piattaforma digitale, accessibile tramite la sezione "cloud" del sito istituzionale dell'ACN, dedicata alla classificazione dei dati e dei servizi della pubblica amministrazione, all'adeguamento delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni ovvero dei servizi cloud erogati da operatore pubblico, nonché alla qualificazione dei servizi cloud;
v) «fornitore di servizi cloud», soggetto, pubblico o privato, che eroga un servizio cloud per le pubbliche amministrazioni, eventualmente anche attraverso l'intermediazione di distributori, rivenditori o prestatori di servizi a valore aggiunto offerti all'utente finale. I distributori, i rivenditori e i prestatori di servizi a valore aggiunto non assumono la qualità di fornitori di servizi cloud a condizione che non determinino le modalità e i mezzi per l'erogazione del servizio cloud;
w) «catena di qualificazione cloud», la relazione tra il servizio cloud per la pubblica amministrazione e la piattaforma attraverso il quale lo stesso è erogato, secondo le modalità descritte in Allegato 4.
x) «FNCS», Framework nazionale per la cybersecurity e la data protection.

Articolo 2
(Finalità, oggetto e ambito di applicazione)

1. Il presente Regolamento, in conformità alle previsioni di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221:
   a) stabilisce i livelli minimi di sicurezza per le pubbliche amministrazioni, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per le pubbliche amministrazioni e delle infrastrutture dei servizi cloud per le pubbliche amministrazioni;
   b) definisce le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per le pubbliche amministrazioni;
   c) individua i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni. A tal fine stabilisce il processo e le modalità per la classificazione dei dati e dei servizi digitali;
   d) definisce le modalità del procedimento di qualificazione dei servizi cloud per le pubbliche

amministrazioni.

2. Il presente Regolamento, inoltre, individua:
   a) le modalità del procedimento di adeguamento delle infrastrutture digitali per le pubbliche amministrazioni e delle infrastrutture dei servizi cloud per le pubbliche amministrazioni;
   b) le modalità del procedimento di adeguamento dei servizi cloud per le pubbliche amministrazioni.

CAPO II
Caratterizzazione e classificazione dei dati e dei servizi digitali della pubblica amministrazione

Articolo 3
(Elenco, caratterizzazione e classificazione dei dati e dei servizi digitali della pubblica amministrazione)

1. Le amministrazioni predispongono e aggiornano un elenco dei propri dati e dei propri servizi digitali, comprensivo di tutti gli elementi necessari alla loro caratterizzazione ai fini della relativa classificazione.
2. I dati e i servizi digitali delle amministrazioni di cui al comma 1 sono classificati, sulla base della loro caratterizzazione, nelle seguenti tre classi:
   a) «ordinari», qualora la loro compromissione non determini i pregiudizi di cui alle lettere b) e c);
   b) «critici», se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;
   c) «strategici», se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale.
3. I dati e i servizi digitali soggetti agli obblighi di cui al decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono classificati come «strategici».
4. I dati e i servizi digitali soggetti agli obblighi di cui al decreto legislativo 18 maggio 2018, n. 65, sono classificati come:
   a) «critici», qualora non siano a valenza nazionale;
   b) «strategici», qualora siano a valenza nazionale.
5. I dati e i servizi digitali di cui ai commi 3 e 4 non sono oggetto dell'elencazione di cui al comma 1.
6. I servizi digitali non ancora classificati ai sensi dei commi 1 e 2 del presente articolo non possono essere resi disponibili agli utenti finali.

Articolo 4
(Predisposizione dell'elenco e della classificazione dei dati e dei servizi digitali della pubblica amministrazione)

1. Le modalità per la predisposizione e l'aggiornamento dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3, nonché per la trasmissione all'ACN, sono definite nell'Allegato 1, che costituisce parte integrante del presente Regolamento.
2. Le modalità di cui al comma 1, rese disponibili sulla piattaforma digitale, sono elaborate:
   a) in relazione al rischio e all'evoluzione della minaccia di natura cibernetica;

b) tenuto conto della normativa e degli standard nazionali, europei e internazionali;
c) con riguardo ai rischi per i diritti e le libertà delle persone fisiche, allorché ci si trovi in presenza di dati personali, diversificati rispetto alle tipologie di dati personali coinvolti e alle categorie degli interessati, in particolare se si tratti di dati riconducibili a categorie di soggetti vulnerabili , se si tratti di categorie particolari di dati quali quelle previste dall'articolo 9 del regolamento (UE) 2016/679 o dati personali relativi a condanne penali e reati di cui all'articolo 10 del regolamento (UE) 2016/679.

3. L'ACN aggiorna le modalità di cui al comma 1, su base periodica, almeno una volta ogni due anni, nel rispetto di quanto previsto dal comma 2.

Articolo 5

(Processo di trasmissione dell'elenco e della classificazione dei dati e dei servizi digitali della pubblica amministrazione)

1. Le amministrazioni aggiornano l'elenco e la classificazione dei dati e dei servizi digitali di cui all'articolo 3 e li trasmettono all'ACN con le modalità indicate nell'Allegato 1, almeno una volta ogni due anni o in presenza dei dati e dei servizi digitali ulteriori rispetto a quelli già oggetto di trasmissione e classificazione, nonché a seguito dell'aggiornamento delle modalità di cui all'articolo 4, secondo i termini ivi stabiliti.
2. L'ACN fornisce riscontro circa la conformità dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3 rispetto alle modalità cui all'articolo 4, entro novanta giorni dalla sua ricezione. Il predetto termine può essere prorogato dall'ACN, per una sola volta e fino ad un massimo di ulteriori trenta giorni, qualora sia necessario svolgere degli approfondimenti riguardanti il processo di trasmissione dell'elenco e della classificazione dei dati e dei servizi digitali della pubblica amministrazione.
3. Ove si renda necessario chiedere integrazioni e informazioni aggiuntive all'amministrazione che ha trasmesso l'elenco e la classificazione dei dati e dei servizi digitali di cui all'articolo 3, i termini di cui al comma 2 sono sospesi e ricominciano a decorrere dalla data di ricevimento delle integrazioni e delle informazioni che sono rese entro il termine di trenta giorni dalla richiesta.
4. Al termine della verifica di conformità di cui al comma 2, l'ACN comunica, al domicilio digitale dell'amministrazione:
   a) la convalida della conformità dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3;
   b) la convalida, con prescrizioni, della conformità dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3;
   c) la non convalida, fornendone le motivazioni, della conformità dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3.
5. Nell'ipotesi di cui al comma 4, lettera b), l'amministrazione trasmette all'ACN, entro trenta giorni, l'adeguamento dell'elenco e della classificazione dei dati e dei servizi alle prescrizioni.
6. In assenza di riscontro da parte dell'ACN entro i termini di cui ai commi 2 e 3, l'elenco e la classificazione dei dati e dei servizi si intendono convalidati ai sensi del comma 4, lettera a).

CAPO III
Livelli minimi delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e caratteristiche dei servizi cloud per le pubbliche amministrazioni

Articolo 6

(Criteri per la definizione dei livelli minimi delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e delle caratteristiche dei servizi cloud per le pubbliche amministrazioni)

1. I livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni nonché le caratteristiche dei servizi cloud per le pubbliche amministrazioni, di cui agli articoli 7 e 8, sono definiti dall'ACN anche sulla base del Framework nazionale per la cybersecurity e la data protection.
2. I livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni nonché le caratteristiche dei servizi cloud per le pubbliche amministrazioni, di cui agli articoli 7 e 8, sono aggiornati periodicamente, almeno una volta ogni due anni:
   a) in linea con la classificazione dei dati e dei servizi che devono trattare;
   b) in relazione al rischio e all'evoluzione della minaccia di natura cibernetica;
   c) in considerazione degli schemi di certificazione nazionali ed europei progressivamente adottati;
   d) tenuto conto delle migliori pratiche, delle linee guida, dei quadri di disciplina di riferimento e degli standard nazionali, europei nonché internazionali;
   e) tenuto conto dell'evoluzione delle misure e delle garanzie necessarie ad assicurare un adeguato livello di protezione dei dati personali.

Articolo 7

(Livelli minimi delle infrastrutture digitali per le pubbliche amministrazioni e delle infrastrutture dei servizi cloud per le pubbliche amministrazioni)

1. Le infrastrutture digitali per le pubbliche amministrazioni e le infrastrutture dei servizi cloud per le pubbliche amministrazioni rispettano i livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità definiti nell'Allegato 2, che costituisce parte integrante del presente Regolamento.
2. Per trattare i dati e i servizi digitali classificati ai sensi dell'articolo 3, quali:
   a) «ordinari», le infrastrutture digitali per le pubbliche amministrazioni e le infrastrutture dei servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alla sezione 2 dell'Allegato 2;
   b) «critici», le infrastrutture digitali per le pubbliche amministrazioni e le infrastrutture dei servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alle sezioni 2 e 3 dell'Allegato 2;
   c) «strategici», le infrastrutture digitali per le pubbliche amministrazioni e le infrastrutture dei servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alle sezioni 2, 3 e 4 dell'Allegato 2.
3. I livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità devono essere garantiti interamente dall'infrastruttura digitale ovvero dai componenti di una infrastruttura digitale messi a disposizione da terzi parti e finalizzati all'erogazione di servizi cloud per la pubblica amministrazione e di cui possono avvalersi anche le infrastrutture digitali congiuntamente dal medesimo operatore e dal fornitore dei cd. servizi di *housing*, attraverso accordi dedicati.
4. Le infrastrutture digitali per le pubbliche amministrazioni e le infrastrutture dei servizi cloud per le pubbliche amministrazioni mediante le quali vengono trattati i dati ed erogati servizi digitali soggetti al decreto-legge n. 105 del 2019 rispettano altresì le prescrizioni in materia di

cloud previste dal predetto decreto.

Articolo 8
(Caratteristiche dei servizi cloud per le pubbliche amministrazioni)

1. I servizi cloud per le pubbliche amministrazioni possiedono le caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità definite nell'Allegato 3, che costituisce parte integrante del presente Regolamento.
2. Per trattare i dati e i servizi digitali classificati ai sensi dell'articolo 3, quali:
   a) «ordinari», i servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alla sezione 2 dell'Allegato 3;
   b) «critici», i servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alle sezioni 2 e 3 dell'Allegato 3;
   c) «strategici», i servizi cloud per le pubbliche amministrazioni devono rispettare i livelli minimi di cui alle sezioni 2, 3 e 4 dell'Allegato 3.
3. I servizi cloud per le pubbliche amministrazioni che trattano dati ed erogano servizi digitali soggetti al decreto-legge n. 105 del 2019, rispettano altresì le prescrizioni in materia di cloud previste dal predetto decreto.

CAPO IV
Migrazione dei dati e dei servizi digitali della pubblica amministrazione

Articolo 9
(Criteri per la migrazione dei dati e dei servizi digitali della pubblica amministrazione)

1. Le amministrazioni, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano, in conformità alle previsioni dell'articolo 33-*septies*, commi 1 e 1-*bis*, del decreto-legge n. 179 del 2012 i dati e servizi digitali verso le infrastrutture digitali per le pubblica amministrazione che, all'esito del processo di adeguamento di cui all'articolo 12, rispettano, in relazione alla classificazione di cui all'articolo 3, i livelli minimi di cui all'articolo 7 e i requisiti di cui al medesimo articolo 12 ovvero verso i servizi cloud, adeguati ai sensi dell'articolo 15, o qualificati ai sensi dell'articolo 17, che, in relazione alla classificazione di cui all'articolo 3, rispettano le caratteristiche di cui all'articolo 8 e i requisiti di cui agli articoli 15 e 17.
2. La migrazione dei dati e dei servizi digitali soggetti agli obblighi di cui al decreto-legge n. 105 del 2019 e al decreto legislativo n. 65 del 2018, ai sensi del comma 1, avviene anche nel rispetto delle previsioni dei suddetti decreti.

Articolo 10
(Modalità per la predisposizione e aggiornamento del piano di migrazione dei dati e dei servizi digitali)

1. Le amministrazioni, all'esito del processo di trasferimento dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 5, predispongono il piano di migrazione dei loro dati e servizi digitali secondo il modello adottato dal Dipartimento per la trasformazione digitale, d'intesa con l'ACN.
2. Il modello di cui al comma 1 è reso disponibile, sulla piattaforma digitale e tramite i canali di comunicazione del Dipartimento per la trasformazione digitale e si applica nel rispetto delle

previsioni di cui all'articolo 27; qualora se ne ravvisi la necessità, può essere aggiornato secondo le modalità del medesimo comma 1.

3. In presenza di dati e servizi digitali ulteriori rispetto a quelli già precedentemente classificati e comunicati con le modalità previste nel successivo articolo 11, le amministrazioni, previo aggiornamento dell'elenco e della classificazione dei dati e servizi digitali di cui all'articolo 3, procedono alla predisposizione del nuovo piano di migrazione in aggiornamento ai piani di migrazione di cui al comma 1.

Articolo 11
(Modalità e termini per la migrazione dei dati e dei servizi digitali)

1. Le amministrazioni, anche ai fini della verifica degli obblighi previsti dall'articolo 33-*septies* del decreto-legge, n. 179 del 2012, trasmettono i piani di migrazione al Dipartimento per la trasformazione digitale e all'AgID, mediante la piattaforma dedicata messa a disposizione dallo stesso Dipartimento per la trasformazione digitale.
2. I piani di migrazione predisposti ai sensi dell'articolo 10, comma 3, sono trasmessi mediante la piattaforma di cui al comma 1.
3. AgID, DTD e ACN accedono alla Piattaforma di cui al comma 1, con le modalità definite attraverso un accordo o una convenzione stipulata tra i medesimi soggetti ai fini di svolgere le attività di competenza rispetto agli obblighi di cui all'articolo 33-septies del decreto-legge n. 179 del 2012. Nelle more della stipula del predetto accordo, AgID e DTD richiedono ad ACN l'elenco di dati e servizi digitali classificati di cui all'articolo 3, ACN richiede a DTD e AGID i piani di migrazione di cui all'articolo 10 per le attività di competenza.
4. Le amministrazioni completano le attività previste dal piano di migrazione, trasmesso ai sensi del comma 1, entro il 30 giugno 2026.
5. Il Dipartimento per la trasformazione digitale, anche avvalendosi di AGID, riscontra la conformità dei piani di migrazione rispetto al modello di cui all'articolo 10, comma 1, entro sessanta giorni dalla data della sua ricezione. Il predetto termine può essere prorogato dal Dipartimento per la trasformazione digitale, per una sola volta e fino ad un massimo di ulteriori sessanta giorni, qualora sia necessario svolgere degli approfondimenti riguardanti il piano di migrazione.
6. Ove si renda necessario chiedere integrazioni e informazioni aggiuntive all'amministrazione che ha trasmesso il piano di migrazione, i termini di cui al comma 4 sono sospesi e ricominciano a decorrere dalla data di ricevimento delle informazioni che sono rese entro il termine di trenta giorni dalla richiesta.
7. Al termine della verifica di conformità di cui al comma 4, il Dipartimento per la trasformazione digitale comunica, al domicilio digitale dell'amministrazione:
   a) la convalida del piano di migrazione;
   b) la convalida, con prescrizioni, del piano di migrazione;
   c) la non convalida, fornendone le motivazioni, del piano di migrazione.
8. Nell'ipotesi di cui al comma 6, lettera b), l'amministrazione trasmette al Dipartimento per la trasformazione digitale entro trenta giorni, l'adeguamento del piano di migrazione alle prescrizioni.
9. In assenza di riscontro da parte del Dipartimento per la trasformazione digitale, entro i termini di cui ai commi 4 e 5, il piano di migrazione si intende convalidato ai sensi del comma 6, lettera a).
10. Nell'ambito delle attività di migrazione di cui al comma 2, le pubbliche amministrazioni possono trattare i propri dati e servizi con le infrastrutture ed i servizi cloud già in uso fino al completamento della migrazione, in caso di piano di migrazione convalidato e, comunque, non oltre il 30 giugno 2026.

CAPO V
Adeguamento delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e qualificazione dei servizi cloud per le pubbliche amministrazioni

Articolo 12
(Adeguamento delle infrastrutture digitali per le pubbliche amministrazioni e delle infrastrutture dei servizi cloud per le pubbliche amministrazioni)

1. I requisiti di adeguamento delle infrastrutture digitali ovvero delle infrastrutture dei servizi cloud per le pubbliche amministrazioni sono suddivisi nei seguenti quattro livelli:
   a) infrastruttura di livello 1 (AI1);
   b) infrastruttura di livello 2 (AI2);
   c) infrastruttura di livello 3 (AI3);
   d) infrastruttura di livello 4 (AI4).
2. I requisiti di adeguamento di cui al comma 1 sono elaborati:
   a) in relazione al rischio e all'evoluzione della minaccia tecnica di natura cibernetica;
   b) tenuto conto della normativa e degli standard nazionali, europei e internazionali;
   c) in considerazione degli schemi di certificazione nazionali ed europei progressivamente adottati;
   d) tenuto conto delle migliori pratiche, delle linee guida, dei quadri di disciplina di riferimento di settore.
3. Al fine dell'adeguamento:
   a) al livello 1 (AI1) di cui al comma 1, l'infrastruttura digitale per le pubbliche amministrazioni ovvero l'infrastruttura dei servizi cloud per le pubbliche amministrazioni deve rispettare i requisiti elencati nella sezione 6 dell'Allegato 4, che costituisce parte integrante del presente Regolamento;
   b) al livello 2 (AI2) di cui al comma 1, l'infrastruttura digitale per le pubbliche amministrazioni ovvero l'infrastruttura dei servizi cloud per le pubbliche amministrazioni deve rispettare i requisiti elencati nella sezione 7 dell'Allegato 4;
   c) al livello 3 (AI3) di cui al comma 1, l'infrastruttura digitale per le pubbliche amministrazioni ovvero l'infrastruttura dei servizi cloud per le pubbliche amministrazioni deve rispettare i requisiti elencati nella sezione 8 dell'Allegato 4;
   d) al livello 4 (AI4) di cui al comma 1, l'infrastruttura digitale per le pubbliche amministrazioni ovvero l'infrastruttura dei servizi cloud per le pubbliche amministrazioni deve rispettare i requisiti elencati nella sezione 9 dell'Allegato 4.
4. I dati e i servizi digitali classificati, ai sensi dell'articolo 3, quali:
   a) «ordinari», sono erogati tramite infrastrutture digitali per le pubbliche amministrazioni ovvero infrastrutture dei servizi cloud per le pubbliche amministrazioni accreditate nell'ambito delle tipologie di cui al comma 1, lettere a), b), c) e d);
   b) «critici», sono erogati tramite infrastrutture digitali per le pubbliche amministrazioni ovvero infrastrutture dei servizi cloud per le pubbliche amministrazioni accreditate nell'ambito delle tipologie di cui al comma 1, lettere b), c) e d);
   c) «strategici», sono erogati tramite infrastrutture digitali per le pubbliche amministrazioni ovvero infrastrutture dei servizi cloud per le pubbliche amministrazioni accreditate nell'ambito delle tipologie di cui al comma 1, lettere c) e d).

Articolo 13

(Modalità e termini per l'adeguamento delle infrastrutture digitali per le pubbliche amministrazioni)

1. A seguito delle attività di adeguamento di cui all'articolo 12, gli operatori di infrastrutture digitali sottoscrivono e trasmettono all'ACN una relazione di conformità ai livelli minimi di cui all'articolo 7 e ai requisiti di cui all'articolo 12, predisposta sulla base del modello reso disponibile sulla piattaforma digitale. Tale previsione si applica nel rispetto delle previsioni di cui all'articolo 27.
2. La relazione di conformità ai fini dell'adeguamento di cui al comma 1 e ai fini della promozione di cui al comma 8, resa ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, è sottoscritta dal legale rappresentante dell'operatore dell'infrastruttura digitale o da un suo delegato ed è presentata telematicamente nel rispetto delle previsioni di cui all'articolo 65, del decreto legislativo 7 marzo 2005, n. 82.
3. Salvo motivata richiesta di non pubblicazione dell'operatore di infrastrutture digitali, soggetta alla valutazione dell'ACN, l'infrastruttura digitale per le pubbliche amministrazioni viene pubblicata nel catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, con l'indicazione "infrastruttura digitale adeguata".
4. Il catalogo, reso disponibile sulla piattaforma digitale, è aggiornato dall'ACN entro trenta giorni dalla ricezione della relazione di conformità di cui al comma 1 fatta salva la possibilità per la stessa ACN di chiedere modifiche e integrazioni della relazione che presenti carenze formali. In tale ultimo caso, il termine di trenta giorni decorre dalla ricezione, da parte di ACN, della documentazione recante le modifiche e le integrazioni richieste.
5. La validità dell'adeguamento decorre:
    a. per i casi di cui al comma 3, dal momento in cui l'ACN riscontra la richiesta di non pubblicazione di cui al medesimo comma;
    b. per i casi di cui al comma 4, dalla data di pubblicazione nel catalogo.
6. In caso di ricorso a servizi di *housing*, la relazione di conformità reca le evidenze dei requisiti di competenza delle terze parti, con l'indicazione del riferimento univoco, se presente, al catalogo di cui al comma 4, della relativa infrastruttura digitale per le pubbliche amministrazioni. Tale indicazione è obbligatoria per le relazioni di conformità inviate a partire dal 01/02/2025.
7. Qualora siano realizzate modifiche sostanziali delle modalità di adozione dei livelli minimi di cui all'articolo 7 e dei requisiti di cui all'articolo 12, l'operatore di infrastrutture digitali ne comunica, tempestivamente e senza ingiustificato ritardo, le relative modalità all'ACN, ai sensi del presente articolo, aggiornando, in ogni caso, la predetta relazione di conformità almeno ogni trentasei mesi.
8. La richiesta di passaggio di un'infrastruttura digitale per le pubbliche amministrazioni ad un diverso livello di adeguamento ("promozione") ai sensi dell'articolo 12 avviene con le medesime modalità per l'adeguamento definite nel presente articolo.

Articolo 14

(Modalità di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni)

1. Ai fini dell'adeguamento di un'infrastruttura dei servizi cloud per le pubbliche amministrazioni, gli operatori di infrastrutture digitali sottoscrivono e trasmettono all'ACN una relazione di conformità ai requisiti di cui all'articolo 12 e ai livelli minimi di cui all'articolo 7, predisposta sulla base del modello reso disponibile sulla piattaforma digitale. Tale previsione si applica nel rispetto delle previsioni di cui all'articolo 27.
2. La relazione di conformità ai fini dell'adeguamento di cui al comma 1 e ai fini della promozione di cui al comma 8, resa ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, è sottoscritta dal legale rappresentante dell'operatore dell'infrastrutture digitale o

da un suo delegato ed è presentata telematicamente nel rispetto delle previsioni di cui all'articolo 65, del decreto legislativo 7 marzo 2005, n. 82.

3. Salvo motivata richiesta di non pubblicazione dell'operatore di infrastrutture digitali, soggetta alla valutazione dell'ACN, l'infrastruttura dei servizi cloud per le pubbliche amministrazioni viene pubblicata nel catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, con l'indicazione "infrastruttura dei servizi cloud adeguata".
4. Il catalogo, reso disponibile sulla piattaforma digitale, è aggiornato dall'ACN entro trenta giorni dalla ricezione della relazione di conformità di cui al comma 1, fatta salva la possibilità per la stessa ACN di chiedere modifiche e integrazioni della relazione che presenti carenze formali. In tale ultimo caso, il termine di trenta giorni decorre dalla ricezione, da parte di ACN, della documentazione recante le modifiche e le integrazioni richieste.
5. La validità dell'adeguamento decorre:
    a. per i casi di cui al comma 3, dal momento l'ACN riscontra la richiesta di non pubblicazione di cui al medesimo comma;
    b. per i casi di cui al comma 4, dalla data di pubblicazione nel catalogo.
6. In caso di ricorso a servizi di *housing*, la relazione di conformità reca le evidenze dei requisiti di competenza delle terze parti, con l'indicazione del riferimento univoco, se presente, al catalogo di cui al comma 4, della relativa infrastruttura dei servizi cloud per le pubbliche amministrazioni. Tale indicazione è obbligatoria per le relazioni di conformità inviate a partire dal 01/02/2025.
7. Qualora siano realizzate modifiche sostanziali delle modalità di adozione dei livelli minimi di cui all'Allegato 2, l'operatore dell'infrastruttura digitale ne comunica, tempestivamente e senza ingiustificato ritardo, le relative modalità all'ACN ai sensi del presente articolo, aggiornando, in ogni caso, la predetta relazione di conformità almeno ogni trentasei mesi.
8. La richiesta di passaggio di un'infrastruttura dei servizi cloud per le pubbliche amministrazioni ad un diverso livello di adeguamento ("promozione") ai sensi dell'articolo 12, avviene con le medesime modalità per l'adeguamento definite nel presente articolo.

Articolo 15
(Adeguamento dei servizi cloud per le pubbliche amministrazioni)

1. I servizi cloud per le pubbliche amministrazioni erogati da un soggetto pubblico, da società in house, ovvero, per espressa previsione normativa, da società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, sono sottoposti al processo di adeguamento.
2. I servizi cloud per le pubbliche amministrazioni sono suddivisi nei seguenti quattro livelli:
    a) cloud di livello 1 (AC1);
    b) cloud di livello 2 (AC2);
    c) cloud di livello 3 (AC3);
    d) cloud di livello 4 (AC4).
3. I requisiti corrispondenti ai livelli di cui al comma 2 sono elaborati:
    a) in relazione al rischio e all'evoluzione della minaccia tecnica di natura cibernetica;
    b) tenuto conto della normativa e degli standard nazionali, europei e internazionali;
    c) in considerazione degli schemi di certificazione nazionali ed europei progressivamente adottati;
    d) tenuto conto delle migliori pratiche, delle linee guida, dei quadri di disciplina di riferimento di settore.
4. Al fine dell'adeguamento:
    a) al livello 1 (AC1) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 2 dell'Allegato 4;

b) al livello 2 (AC2) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 3 dell'Allegato 4;
c) al livello 3 (AC3) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 4 dell'Allegato 4;
d) al livello 4 (AC4) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 5 dell'Allegato 4.

5. I dati e i servizi digitali classificati, ai sensi dell'articolo 3, quali:
   a) «ordinari» possono essere erogati tramite servizi cloud adeguati nell'ambito delle tipologie di cui al comma 1, lettere a) b) c) e d);
   b) «critici» possono essere erogati tramite servizi cloud adeguati nell'ambito delle tipologie di cui al comma 1, lettere b), c) e d);
   c) «strategici» possono essere erogati tramite servizi cloud adeguati nell'ambito delle tipologie di cui al comma 1, lettere c) e d).

Articolo 16

(Modalità e termini per l'adeguamento dei servizi cloud per le pubbliche amministrazioni)

1. I fornitori dei servizi cloud di cui all'articolo 15, comma 1, sottoscrivono e trasmettono all'ACN una relazione di conformità ai requisiti di cui al medesimo articolo 15 e ai livelli minimi di cui all'articolo 8, predisposta sulla base del modello reso disponibile sulla piattaforma digitale nel rispetto delle previsioni di cui all'articolo 27.
2. La relazione di conformità ai fini dell'adeguamento di cui al comma 1 e ai fini della promozione di cui al comma 8, resa ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, è sottoscritta dal legale rappresentante del fornitore di servizi cloud o da un suo delegato ed è presentata telematicamente nel rispetto delle previsioni di cui all'articolo 65, del decreto legislativo 7 marzo 2005, n. 82.
3. Salvo motivata richiesta di non pubblicazione del fornitore di servizi cloud, soggetta alla valutazione dell'ACN, il servizio cloud per le pubbliche amministrazioni viene pubblicato nel catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, con l'indicazione "servizio cloud per le pubbliche amministrazioni adeguato".
4. Il catalogo, reso disponibile sulla piattaforma digitale, è aggiornato dall'ACN entro trenta giorni dalla ricezione della relazione di conformità di cui al comma 1, fatta salva la possibilità per la stessa ACN di chiedere modifiche e integrazioni della relazione che presenti carenze formali. In tale ultimo caso, il termine di trenta giorni decorre dalla ricezione, da parte di ACN, della documentazione recante le modifiche e le integrazioni richieste.
5. La validità dell'adeguamento decorre:
   a. per i casi di cui al comma 3, dal momento l'ACN riscontra la richiesta di non pubblicazione di cui al medesimo comma;
   b. per i casi di cui al comma 4, dalla data di pubblicazione nel catalogo.
6. In caso di ricorso a infrastrutture di prossimità, la relazione di conformità reca le evidenze dell'analisi volta a riscontrare l'assenza di detrimento delle caratteristiche di cui all'articolo 8 e dei requisiti di cui all'articolo 15, anche sulla scorta delle prescrizioni di cui al paragrafo 2.4 dell'allegato 4, con l'indicazione delle relative infrastrutture digitali per le pubbliche amministrazioni.
7. Qualora siano realizzate modifiche sostanziali delle modalità di adozione delle caratteristiche di cui all'Allegato 3, il fornitore di servizi cloud per le pubbliche amministrazioni ne comunica, tempestivamente e senza ingiustificato ritardo, le relative modalità all'ACN ai sensi del presente articolo, aggiornando, in ogni caso, la predetta relazione di conformità almeno ogni trentasei mesi.
8. La richiesta di passaggio di un servizio cloud per le pubbliche amministrazioni ad un diverso

livello di adeguamento ai sensi dell'articolo 15 ("promozione") avviene con le medesime modalità per l'adeguamento definite nel presente articolo.

Articolo 17
(Qualificazione dei servizi cloud per le pubbliche amministrazioni)

1. La qualificazione dei servizi cloud per le pubbliche amministrazioni a cui sono tenuti i fornitori dei servizi cloud diversi da quelli di cui all'articolo 15, comma 1, è articolata nei seguenti quattro livelli:
   a) cloud di livello 1 (QC1);
   b) cloud di livello 2 (QC2);
   c) cloud di livello 3 (QC3);
   d) cloud di livello 4 (QC4).
2. I requisiti corrispondenti ai livelli di cui al comma 1 sono elaborati:
   a) in relazione al rischio e all'evoluzione della minaccia tecnica di natura cibernetica;
   b) tenuto conto della normativa e degli standard nazionali, europei e internazionali;
   c) in considerazione degli schemi di certificazione nazionali ed europei progressivamente adottati;
   d) tenuto conto delle migliori pratiche, delle linee guida, dei quadri di disciplina di riferimento e degli standard nazionali, europei nonché internazionali.
3. Al fine della qualificazione:
   a) al livello 1 (QC1) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 2 dell'Allegato 4;
   b) al livello 2 (QC2) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 3 dell'Allegato 4;
   c) al livello 3 (QC3) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 4 dell'Allegato 4;
   d) al livello 4 (QC4) di cui al comma 1, il servizio cloud deve rispettare i requisiti elencati nella sezione 5 dell'Allegato 4.
4. I dati e i servizi digitali classificati, ai sensi dell'articolo 3, quali:
   a) «ordinari» possono essere erogati tramite servizi cloud accreditati nell'ambito delle tipologie di cui al comma 1, lettere a), b), c) e d);
   b) «critici» possono essere erogati tramite servizi cloud accreditati nell'ambito delle tipologie di cui al comma 1, lettere b), c) e d);
   c) «strategici» possono essere erogati tramite servizi cloud accreditati nell'ambito delle tipologie di cui al comma 1, lettere c) e d).

Articolo 18
(Domanda di qualificazione dei servizi cloud per le pubbliche amministrazioni)

1. Le domande di qualificazione e quelle di promozione di cui al comma 4, rese ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, sono sottoscritte dal legale rappresentante del fornitore dei servizi cloud o da un suo delegato e sono presentate telematicamente nel rispetto delle previsioni di cui all'articolo 65, del decreto legislativo 7 marzo 2005, n. 82.
2. I fornitori dei servizi cloud diversi da quelli di cui all'articolo 15, comma 1, trasmettono telematicamente le domande di cui al comma 1 con le informazioni necessarie, la documentazione a corredo, laddove richiesto, e le modalità indicate sulla piattaforma digitale nel rispetto delle previsioni di cui all'articolo 27, elaborate in forma graduale in accordo al

livello di qualifica richiesto.

3. Le informazioni necessarie di cui al comma 2, includono, almeno:
   a) la tipologia di qualificazione richiesta di cui all'articolo 17;
   b) il servizio cloud sottostante ovvero, in caso erogazione senza il ricorso ad altri servizi cloud, l'infrastruttura digitale ovvero l'infrastruttura dei servizi cloud utilizzata, ai sensi dell'articolo 20;
   c) la descrizione dei servizi cloud per i quali viene richiesta la qualificazione;
   d) l'indicazione dei requisiti posseduti ai fini della qualificazione richiesta e la relativa documentazione;
   e) la specifica e l'esito delle attività di verifica della sicurezza effettuate dal fornitore sul servizio oggetto di qualifica;
   f) nel caso di richieste a partire dal livello 3 di qualificazione, la descrizione degli elementi architetturali dell'infrastruttura o del servizio cloud.
4. La richiesta di passaggio di un servizio cloud per le pubbliche amministrazioni ad un diverso livello di qualificazione ("promozione") ai sensi dell'articolo 15, avviene con le medesime modalità per la qualificazione definite nel presente articolo.
5. In caso di ricorso a infrastrutture di prossimità, la relazione di conformità reca le evidenze dell'analisi volta a riscontrare l'assenza di detrimento delle caratteristiche di cui all'articolo 8 e dei requisiti di cui all'articolo 17, anche sulla scorta delle prescrizioni di cui al paragrafo 2.4 dell'Allegato 4, con l'indicazione delle relative infrastrutture digitali per le pubbliche amministrazioni.

Articolo 19
(Modalità di qualificazione dei servizi cloud per le pubbliche amministrazioni)

1. Entro sessanta giorni dalla ricezione di una domanda di qualificazione da parte di un soggetto richiedente, trasmessa secondo le modalità di cui all'articolo 18, l'ACN verifica la conformità ai requisiti previsti per i livelli di qualificazione di cui all'articolo 17, e ai livelli minimi di cui all'articolo 8, in relazione alla tipologia di qualificazione richiesta.
2. Nell'ambito della verifica di conformità di cui al comma 1, l'ACN può:
   a) formulare quesiti;
   b) richiedere integrazioni, informazioni aggiuntive e la produzione di ulteriore documentazione;
   c) svolgere accertamenti di carattere tecnico, incluse le verifiche di sicurezza mirate ad accertare la presenza di vulnerabilità nei sistemi, anche mediante accesso all'infrastruttura fisica e logica dell'infrastruttura dei servizi cloud ovvero del servizio cloud;
   d) audire il soggetto richiedente.
3. Qualora sia necessario svolgere approfondimenti, ivi inclusi quelli di cui al comma 2, riguardanti aspetti tecnici nell'ambito della verifica di conformità, il termine di cui al comma 1 è prorogato fino a trenta giorni, prorogabili ulteriormente di trenta giorni in casi di particolare complessità.
4. Ove si renda necessario chiedere informazioni e documentazione al soggetto richiedente la qualificazione, ivi incluse quelle di cui al comma 2, i termini sono sospesi e ricominciano a decorrere dalla data di ricevimento delle informazioni e della documentazione, che sono rese entro il termine di quindici giorni dalla richiesta, decorsi i quali l'istanza si intende non accolta.
5. Al termine della verifica di conformità di cui al presente articolo, l'ACN comunica, entro quindici giorni, al domicilio digitale del soggetto richiedente:
   a) il rigetto, fornendone le motivazioni, della qualificazione del servizio cloud;
   b) il rilascio, con condizioni motivate, della qualificazione del servizio cloud, specificandone

la durata;

c) il rilascio, senza condizioni, della qualificazione del servizio cloud, specificandone la durata.

6. La qualificazione ha una durata massima pari a trentasei mesi.
7. L'ACN, nell'ipotesi in cui intende procedere nei sensi di cui al comma 5, lettera a), prima della formale adozione del provvedimento negativo, comunica al soggetto richiedente, entro il termine di cui al medesimo comma 5, i motivi che ostano all'accoglimento della domanda. Il soggetto richiedente, entro il termine di dieci giorni dal ricevimento della comunicazione, può presentare le proprie osservazioni, eventualmente corredate da documentazione a supporto. La comunicazione di ACN sospende i termini di conclusione del procedimento, che ricominciano a decorrere dieci giorni dopo la presentazione delle osservazioni o, in mancanza delle stesse, dalla scadenza dei termini previsti per il soggetto richiedente. Qualora il soggetto richiedente abbia presentato osservazioni, del loro eventuale mancato accoglimento ACN è tenuta a dare ragione nella motivazione del provvedimento finale di rigetto indicando, se ve ne sono, i soli motivi ostativi ulteriori che sono conseguenza delle osservazioni.
8. L'ACN, nelle ipotesi di cui al comma 5, lettere b) e c), pubblica il servizio cloud per le pubbliche amministrazioni nel catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, con l'indicazione "servizio cloud per le pubbliche amministrazioni qualificato con condizioni" ovvero "servizio cloud per le pubbliche amministrazioni qualificato". Il catalogo, reso disponibile sulla piattaforma digitale, è aggiornato dall'ACN entro quindici giorni dal termine della verifica di conformità di cui al presente articolo.
9. Tenuto conto dei termini di conclusione del procedimento di qualifica di cui al presente articolo, ove sia necessario rinnovare la qualificazione di un servizio cloud, le relative istanze sono presentate novanta giorni prima della scadenza della stessa qualifica secondo le medesime modalità previste nel presente articolo. L'ACN, in questo caso, potrà autorizzare il soggetto richiedente ad operare in continuità fino alla data di conclusione del procedimento di rinnovo. Il soggetto richiedente informa di tale periodo di transizione e del procedimento in corso i soggetti con i quali intende stipulare contratti connessi all'applicazione del presente Regolamento.

Articolo 20
(Monitoraggio delle infrastrutture digitali, delle infrastrutture dei servizi cloud e dei servizi cloud per le pubbliche amministrazioni)

1. Successivamente all'adeguamento di cui agli articoli 13, 14 e 16 ovvero al rilascio delle qualifiche ai sensi dell'articolo 18, l'ACN può effettuare verifiche per accertare il possesso e il mantenimento dei requisiti di cui agli articoli 7, 8, 12, 15 e 17 in relazione alla tipologia e al livello di adeguamento o di qualificazione, con le modalità di cui all'articolo 19, comma 2.
2. Laddove, successivamente alle verifiche effettuate ai sensi del comma 1, dovessero emergere profili relativi al mancato rispetto dei requisiti prescritti dal presente Regolamento, anche a seguito degli eventuali supplementi istruttori condotti con la collaborazione dei soggetti interessati, l'ACN richiede, prima dell'avvio delle procedure di revoca, all'operatore di infrastrutture digitali ovvero al fornitore di servizi cloud di garantire il rispetto dei suddetti requisiti entro quarantacinque giorni dalla stessa richiesta fatte salve specifiche, diverse, esigenze per le quali sia necessario prevedere un termine diverso.
3. A seguito della richiesta di cui al comma 2, e fino al positivo accertamento, da parte dell'ACN, dell'avvenuto adempimento della stessa, l'operatore di infrastrutture digitali ovvero il fornitore di servizi cloud ha l'obbligo di comunicare, ai soggetti con i quali ha già in essere o con i quali intende stipulare contratti connessi all'applicazione del presente Regolamento, di essere sottoposto a verifica da parte dell'ACN. Durante il periodo di verifica l'operatore garantisce

comunque la continuità delle prestazioni previste dai contratti in essere.

4. Al termine del periodo di cui al comma 2, l'ACN:
   a) in caso di adempimento da parte dell'operatore, comunica allo stesso l'esito positivo delle verifiche effettuate. L'operatore a sua volta ne dà informazione ai soggetti con i quali ha in essere contratti connessi all'applicazione del presente Regolamento;
   b) in caso di inadempimento, attiva le procedure previste dagli articoli 21 e 23.

Articolo 21
(Revoca della qualifica e dichiarazione di inadeguatezza)

1. Nelle ipotesi previste dall'articolo 20, comma 4, lettera b), l'ACN dispone la revoca della qualificazione ovvero dichiara l'inadeguatezza dell'infrastruttura digitale per le pubbliche amministrazioni, dell'infrastruttura per i servizi cloud per le pubbliche amministrazioni o del servizio cloud per le pubbliche amministrazioni di cui all'articolo 15.
2. Contestualmente alla revoca o alla dichiarazione di inadeguatezza di cui al comma 1, comunicate al domicilio digitale del soggetto interessato, l'ACN contrassegna l'infrastruttura digitale per le pubbliche amministrazioni, l'infrastruttura per i servizi cloud per le pubbliche amministrazioni ovvero il servizio cloud per le pubbliche amministrazioni pubblicata sul catalogo delle infrastrutture e dei servizi cloud per le pubbliche amministrazioni, con l'indicazione "infrastruttura/servizio inadeguato" ovvero "qualificazione revocata".
3. I provvedimenti di revoca e le dichiarazioni di inadeguatezza di cui al comma 1 sono pubblicati, in ogni caso, sulla piattaforma digitale.
4. L'operatore di infrastrutture digitali e il fornitore di servizi cloud, a seguito della revoca o della dichiarazione di inadeguatezza di cui al comma 1, devono:
   a) informare, senza ritardo, dell'intervenuta revoca o dichiarazione di inadeguatezza le eventuali amministrazioni clienti;
   b) supportare le eventuali amministrazioni clienti nelle attività di migrazione verso altro operatore di infrastruttura digitale ovvero fornitore di servizi cloud, scelto dalla medesima amministrazione cliente, garantendo un'agevole esportazione dei dati e fornendo la piena collaborazione per l'instaurazione dei flussi di comunicazione e migrazione verso l'infrastruttura del nuovo fornitore, per il trasferimento automatico dei dati e dei servizi previsti;
   c) eliminare definitivamente, all'esito della positiva migrazione, tutti i dati dell'amministrazione eventualmente memorizzati o ancora nella propria disponibilità.
5. Le amministrazioni, in caso di intervenuta revoca o dichiarazione di inadeguatezza di cui al comma 1, possono continuare a fruire del servizio revocato per un periodo massimo di sei mesi decorrenti dalla data di revoca o dalla dichiarazione di inadeguatezza, eventualmente prorogabili, su specifica istanza, in presenza di documentati elementi di complessità tecnica, fatta salva ogni diversa determinazione dell'ACN.

Capo VI
Disposizioni finali, transitorie, entrata in vigore e applicazione del Regolamento

Articolo 22
(Trattamento dei dati personali)

1. Le amministrazioni sono titolari dei trattamenti di dati personali effettuati nell'ambito delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e dei servizi cloud per le pubbliche amministrazioni.

2. Gli operatori di infrastrutture digitali, i fornitori di servizi cloud e gli ulteriori soggetti coinvolti nei trattamenti di dati personali di cui al comma 1 o nelle attività di migrazione dei dati e dei servizi digitali della pubblica amministrazione di cui al capo IV, nonché i soggetti di cui questi si avvalgono per l'esecuzione di specifiche attività di trattamento per conto delle amministrazioni, operano come responsabili del trattamento ai sensi dell'articolo 28 del regolamento (UE) 2016/679.
3. I soggetti di cui al comma 2 adottano misure tecniche e organizzative idonee a garantire una tempestiva e adeguata informazione delle amministrazioni in caso di violazione dei dati personali, ai sensi dell'articolo 33, paragrafo 2, del regolamento (UE) 2016/679.
4. Il ricorso ad altri responsabili del trattamento da parte dei soggetti di cui al comma 2 è disciplinato in conformità all'articolo 28, paragrafi 2 e 4, del regolamento (UE) 2016/679, prevedendo misure tecniche e organizzative per fornire alle amministrazioni idonei strumenti di controllo delle attività di trattamento effettuate sotto la propria responsabilità.
5. In caso di trasferimento di dati personali al di fuori dello Spazio economico europeo, i responsabili del trattamento di cui ai commi 2 e 4 sono tenuti ad attenersi alle istruzioni delle amministrazioni impartite ai sensi dell'articolo 28, paragrafo 3, lettera a), del regolamento (UE) 2016/679 e a mettere a disposizione delle stesse ogni informazione necessaria per valutare l'effettività delle misure appropriate poste in essere ai sensi del capo V del regolamento (UE) 2016/679.
6. Fermi restando la competenza del Garante per la protezione dei dati personali per le violazioni delle disposizioni contenute nel presente articolo e gli obblighi di comunicazione allo stesso Garante da parte dei soggetti di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica al Garante le evidenze, di cui venga a conoscenza, relative a possibili violazioni di dati persona

Articolo 23
(Segnalazioni all'Agenzia per l'Italia digitale)

1. L'ACN, in tutti i casi in cui rilevi il mancato rispetto, da parte delle Amministrazioni, delle previsioni di cui al presente Regolamento, segnala la violazione riscontrata all'Agenzia per l'Italia digitale al fine dell'applicazione dell'articolo 33-septies, comma 4-quinquies, del decreto-legge n. 179 del 2012.

Articolo 24
(Passaggio al regime ordinario)

1. A decorrere dalla data di entra in vigore del presente Regolamento:
   a) le infrastrutture dei servizi cloud in possesso di qualifica valida, rilasciata dall'ACN entro la data di applicazione del presente Regolamento, si intendono adeguate, ai sensi dell'articolo 12, con il medesimo livello e fino alla scadenza previsti dalla qualifica ottenuta;
   b) i servizi cloud in possesso di qualifica valida, rilasciata dall'ACN entro la data di applicazione del presente Regolamento, si intendono qualificati, ai sensi dell'articolo 17, con il medesimo livello e fino alla scadenza previsti della qualifica ottenuta.

Articolo 25
(Disposizioni transitorie)

1. Gli elenchi dei dati e servizi di cui all'articolo 3 e i piani di migrazione di cui all'articolo 10 trasmessi precedentemente all'adozione del presente Regolamento, si intendono trasmessi anche ai fini del presente Regolamento.
2. Gli operatori di infrastrutture digitali che, nella relazione inviata entro il 18 gennaio 2024, di

cui all'articolo 13, comma 2, hanno dichiarato di aver adottato, entro il 30 settembre 2023, la decisione di contrarre rispetto a documentati interventi di adeguamento, di maggiore complessità, ai livelli minimi di cui all'articolo 7 e ai requisiti di cui all'articolo 12, completano le attività di adeguamento entro il 18 ottobre 2024. Fino al completamento delle attività di adeguamento, gli stessi operatori continuano a trattare i propri dati e servizi con le infrastrutture i servizi cloud già in uso.

3. I fornitori di servizi cloud che, nella relazione inviata entro il 18 gennaio 2024 di cui all'articolo 16, comma 2, hanno dichiarato di aver adottato, entro il 30 settembre 2023, la decisione di contrarre rispetto a documentati interventi di adeguamento, di maggiore complessità, ai livelli minimi di cui all'articolo 8 e ai requisiti di cui all'articolo 15, completano le attività di adeguamento entro il 18 ottobre 2024. Fino al completamento delle attività di adeguamento, gli stessi fornitori continuano a trattare i propri dati e servizi con le infrastrutture i servizi cloud già in uso.

Articolo 26
(Abrogazioni)

1. Sono abrogati, a decorrere dalla data di applicazione del presente Regolamento:
   a) Il regolamento adottato dall'Agenzia per l'Italia digitale con Determinazione del 15 dicembre 2021, n. 628;
   b) la determina n. 306 del 18 gennaio 2022, dell'Agenzia per la cybersicurezza nazionale;
   c) la determina n.307 del 18 gennaio 2022, dell'Agenzia per la cybersicurezza nazionale;
   d) Il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 2 gennaio 2023, prot. n. 29;
   e) Il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale dell'8 febbraio 2023, prot. n. 5489;
   f) Il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 28 luglio 2023, prot. n. 20610;
   g) Il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 30 gennaio 2024, prot. n. 2927.

Articolo 27
(Applicazione del Regolamento e dei requisiti)

1. Il presente Regolamento si applica a decorrere dal 1 agosto 2024. Fino a tale data, resta in vigore il regime transitorio previsto dal decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 2 gennaio 2023, prot. n. 29.
2. I requisiti previsti dagli articoli 7, 8, 12, 15 e 17, di cui agli Allegati 2, 3 e 4, si applicano secondo le modalità e i tempi indicati nei medesimi Allegati.
3. Il presente Regolamento è pubblicato sul sito istituzionale dell'Agenzia per la cybersicurezza nazionale (www.acn.gov.it), sulla piattaforma digitale e ne sarà data, altresì, comunicazione tramite pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Firmato digitalmente da: Bruno Frattasi
Data: 27/06/2024 18:27:08

REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, AI SENSI DELL'ARTICOLO 33-SEPTIES, COMMA 4, DEL DECRETO-LEGGE 18 OTTOBRE 2012, N. 179, CONVERTITO, CON MODIFICAZIONI, DALLA LEGGE 17 DICEMBRE 2012, N. 221

ALLEGATO 1

"MODALITA PER LA PREDISPOSIZIONE DELL'ELENCO E DELLA CLASSIFICAZIONE DEI DATI E DEI SERVIZI DELLA PUBBLICA AMMINISTRAZIONE"

1. **Premessa**
   1.1. Il presente Allegato definisce, in conformità alle previsioni di cui all'articolo 4 del Regolamento, le modalità per la predisposizione e l'aggiornamento dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3 del Regolamento, nonché la relativa procedura di trasmissione all'ACN ai fini della verifica di conformità di cui all'articolo 5 del Regolamento.
   1.2. Al fine di agevolare le amministrazioni nella predisposizione dell'elenco e della classificazione dei propri dati e servizi digitali, ACN rende disponibile sulla piattaforma digitale di cui all'articolo 1, comma 1, lettera z), del Regolamento:
      a) elenchi predefiniti di dati e/o servizi, già corredati dalla relativa classificazione, per gruppi omogenei di amministrazioni che la singola amministrazione può modificare o integrare ai sensi del punto 2 del presente Allegato;
      b) questionari e modelli di classificazione per l'eventuale valutazione della classificazione di dati e/o servizi ad integrazione degli elenchi predefiniti e per l'eventuale rivalutazione della classificazione di dati e/o servizi presenti negli elenchi predefiniti.
   1.3. Gli elenchi predefiniti, i modelli e gli algoritmi di classificazione sono aggiornati su base periodica, almeno una volta ogni due anni, secondo le modalità di cui al presente Allegato. Dell'aggiornamento viene data notizia tramite i canali di comunicazione dell'ACN.
   1.4. Al fine di predisporre e aggiornare gli elenchi predefiniti, i questionari e i modelli, l'ACN può avvalersi di gruppi rappresentativi di amministrazioni omogenee. Le amministrazioni individuate dall'ACN per costituire i gruppi rappresentativi di amministrazioni omogenee aderiscono su base volontaria.

2. **Processo di elencazione e classificazione dei dati e dei servizi digitali**
   2.1. Per la predisposizione e l'aggiornamento dell'elenco e della classificazione dei propri dati e servizi digitali, le amministrazioni prendono visione dell'elenco predefinito e della relativa classificazione di cui al punto 1.2, lettera a), sulla piattaforma digitale e, tramite le funzionalità offerte dalla stessa piattaforma digitale, possono:
      a. accettare l'elenco predefinito e la relativa classificazione. In tal caso l'elenco e la classificazione di cui all'articolo 3 del Regolamento si intendono convalidati ai sensi dell'articolo 5, comma 4, lettera a), del medesimo Regolamento;
      b. qualora non trattino tutti i dati e/o i servizi digitali presenti nell'elenco predefinito, modificare l'elenco, eliminando i dati e i servizi che non sono trattati. L'aggiornamento dell'elenco e della classificazione è trasmesso all'ACN, mediante la piattaforma digitale, per la verifica di conformità di cui all'articolo 5, comma 2, del presente Regolamento;
      c. qualora trattino ulteriori dati e/o servizi digitali rispetto a quelli presenti nell'elenco predefinito, integrare l'elenco predefinito e la relativa classificazione. In tal caso l'elenco integrato è trasmesso all'ACN, mediante la piattaforma digitale, unitamente ai questionari per la classificazione di cui al punto 1.2, lettera b), compilati in ogni loro parte per ogni dato e servizio digitale trattato e non presente nell'elenco predefinito. L'elenco integrato e i questionari sono soggetti alla verifica di conformità di cui all'articolo 5, comma 2, del presente Regolamento;
      d. qualora non ritengano coerente la classificazione proposta per dei dati e/o dei servizi digitali presenti nell'elenco predefinito, variare la relativa classificazione. In tal caso l'elenco è trasmesso all'ACN, mediante la piattaforma digitale, unitamente ai questionari di cui al punto 1.2, lettera b), compilati in ogni loro parte per variare la classificazione per ogni dato e servizio trattato e di cui non si ritiene la classificazione proposta coerente. L'elenco e i nuovi questionari sono soggetti alla verifica di conformità di cui all'articolo 5, comma 2, del presente Regolamento.
   2.2. Per motivate e documentate ragioni di natura normativa o tecnica, in deroga a quanto previsto al punto

2.1, le amministrazioni centrali di cui all'articolo 1, comma 1, lettera c), possono presentare telematicamente ad ACN, nel rispetto delle previsioni di cui all'articolo 65, del decreto legislativo 7 marzo 2005, n. 82, l'elencazione e la classificazione dei propri dati e servizi digitali, unitamente alle motivazioni e all'analisi del rischio svolta per addivenire alla classificazione prodotta, secondo il modello reso disponibile tramite i canali di comunicazione dell'ACN.

REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, AI SENSI DELL'ARTICOLO 33-SEPTIES, COMMA 4, DEL DECRETO-LEGGE 18 OTTOBRE 2012, N. 179, CONVERTITO, CON MODIFICAZIONI, DALLA LEGGE 17 DICEMBRE 2012, N. 221

ALLEGATO 2

"LIVELLI MINIMI DI SICUREZZA E AFFIDABILITÀ, CAPACITÀ ELABORATIVA, RISPARMIO ENERGETICO DELLE INFRASTRUTTURE DIGITALI E DELLE INFRASTRUTTURE DEI SERVIZI PER LA PUBBLICA AMMINISTRAZIONE"

Sommario

1. **Premessa e definizioni** 1
2. **Livelli minimi previsti nel caso di dati e servizi ordinari** 2
3. **Livelli minimi previsti nel caso di dati e servizi critici** 10
4. **Livelli minimi previsti nel caso di dati e servizi strategici** 17
5. **Livelli minimi con termini di adozione differiti** 25
6. **Appendice** 27

1. Premessa e definizioni

1.1. Il presente Allegato definisce, in conformità alle previsioni di cui agli articoli 6 e 7 del Regolamento, i livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per le pubbliche amministrazioni e delle infrastrutture dei servizi cloud per le pubbliche amministrazioni che possono ospitare, rispettivamente, servizi e dati digitali della pubblica amministrazione coerentemente con il relativo livello di classificazione di cui all'articolo 3 del Regolamento.

1.2. I livelli minimi sono organizzati sulla base delle sottocategorie del Framework Nazionale per la Cybersecurity e la Data Protection di seguito denominato (FNCS). 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.

1.3. I livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali di cui al presente Allegato si applicano agli ambienti di produzione. I livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità degli ambienti di pre-produzione, test, sviluppo e ad essi assimilabili sono applicati in coerenza con i livelli minimi delle infrastrutture digitali di cui al presente Allegato, eventualmente in relazione ad un'analisi del rischio volta a individuare i potenziali impatti sul servizio e sui relativi dati gestiti ovvero sull'infrastruttura digitale relativa all'ambiente di produzione.

1.4. Ai fini del presente Allegato, si intende per:

a) "Dati dell'amministrazione", dati forniti, conservati, inviati, ricevuti, trattati da o per conto dell'Amministrazione dal soggetto tramite l'Infrastruttura digitale;

b) "Metadata relativi all'amministrazione", dati raccolti, ottenuti o generati dal soggetto, anche in forma derivata, a partire dai dati dell'amministrazione, nell'ambito dell'erogazione e dell'amministrazione dell'Infrastruttura digitale. In tale categoria rientrano, ad esempio la storicizzazione degli eventi dei sistemi e servizi, le configurazioni dei servizi e gli attributi delle risorse dell'amministrazione, derivanti anche dall'utilizzo degli stessi;

c) "Metadata relativi al funzionamento dell'Infrastruttura digitale", dati generati e utilizzati dal soggetto per monitorare e garantire la funzionalità dell'Infrastruttura digitale, non inclusi in Metadata dell'amministrazione o dati dell'amministrazione. In tale categoria di Metadata, che

non devono quindi essere riconducibili a persone, al soggetto e non possono comunque permettere di estrarre - anche in parte - i dati dell'amministrazione, rientrano, ad esempio le metriche sulle performance d'utilizzo, bilanciamento, etc.

d) "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 dipende il funzionamento dell'infrastruttura digitale;

e) "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 servizio cloud, ma di pertinenza dell'operatore dell'infrastruttura digitale, da cui dipende il funzionamento dell'infrastruttura digitale;

f) "catena di approvvigionamento cyber", la catena di approvvigionamento relativa all'Infrastruttura digitale.

1.5. Ad eccezione dell'organizzazione di cybersecurity, il termine "organizzazione", che compare all'interno delle descrizioni delle categorie e sottocategorie, è da intendersi riferito almeno all'infrastruttura o al personale dell'operatore dell'infrastruttura digitale per le pubbliche amministrazioni ovvero dell'infrastrutture dei servizi cloud per le pubbliche amministrazioni preposto alla sua gestione. In aggiunta, il termine "soggetto" è da intendersi nell'accezione di "operatore di infrastruttura digitale".

2. Livelli minimi previsti nel caso di dati e servizi ordinari

2.1 Affidabilità

2.1.1) Alta Affidabilità.

A.AA-01: Disponibilità dell'infrastruttura

1_O. *L'indice di disponibilità dell'Infrastruttura Digitale, riferita alla percentuale di tempo in un anno in cui l'infrastruttura risulta essere accessibile e usabile, deve essere stato almeno pari:*
a. 99,98% al netto dei fermi programmati;
b. 99,6 % comprendendo i fermi programmati.

A.AA-02: Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità

1_O. *Il Centro di elaborazione dati (CED) deve essere dotato di soluzioni hardware e software (apparati di rete e sicurezza, storage, servizi di virtualizzazione, etc.) per la configurazione dei servizi in alta affidabilità. Devono essere inoltre messe a disposizione capability e funzionalità a supporto di configurazioni dei servizi in alta affidabilità quali:*
a. Scelta della replica locale dei dati per un servizio storage;
b. Presenza di servizi di bilanciamento di carico;
c. Meccanismi di anti-affinity per la distribuzione delle istanze computazionali.

2.1.2) Business Continuity e Disaster Recovery.

A.BC-01: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti

1_O. *Provider di infrastruttura: L'infrastruttura digitale è dotata di soluzioni di DR, con caratteristiche coerenti con l'analisi del rischio, e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA.*

2_O. *Con riferimento ai valori di RTO e RPO definiti al punto 1_O, devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 48 ore e RPO 48 ore.*

2.1.3) Governance e processi.

A.GP-01: I Servizi IT sono gestiti conformemente agli standard di settore

1_O. *Sono adottati processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2.*

A.GP-02: È garantito il rispetto degli indicatori di servizio obbligatori

1_O. *Per il Centro di elaborazione dati (CED), il soggetto deve garantire il supporto tecnico per emergenze con:*

a. una copertura di 24 ore al giorno, 7 giorni a settimana per tutto l'anno;

b. un tempo massimo di risposta agli incidenti (inteso come tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta da parte del soggetto) pari a 1 ora.

2_O. *Il soggetto deve garantire, per i servizi del Centro di elaborazione dati (CED) offerti, un supporto tecnico con le seguenti caratteristiche:*

a. fornito, almeno in lingua inglese, dalle 08.00 alle 18.00 (ora italiana) nei giorni lavorativi

b. accessibile preferenzialmente tramite i seguenti canali: recapito telefonico ed e-mail.

Su richiesta dell'Amministrazione, il servizio di supporto è fornito almeno in lingua italiana.

2.1.4) Performance e Scalabilità.

A.PS-01: Sono garantite caratteristiche minime di connettività

1_O. *Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite:*

a. bandwidth di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.

2.2 Capacità Elaborativa

2.2.1) Capacità Elaborativa.

CE.CE-01: Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore

1_O. *La capacità elaborativa dell'Infrastruttura Digitale è gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.*

2.3 Data Center Security

2.3.1) Data Center Security.

S.DC-01: I Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale

1_O. *Il soggetto garantisce il presidio operativo all'interno del Data Center per 24 ore al giorno, 7 giorni a settimana per tutto l'anno.*

2_O. *Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.*

3_O. *Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.*

4_O. *Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.*

5_O. *Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).*

S.DC-02: Sono adottate misure di sicurezza fisica e ambientale

1_O. *Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste policy e procedure dovranno essere riviste su base almeno annuale.*

2_O. *Sono implementati, manutenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato.*

3_O. *Sono implementati, mantenuti e adottati, all'interno dei Data Center, i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.*

2.4 Risparmio Energetico

2.4.1) Risparmio Energetico.

RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore

1_O. *Il soggetto ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti, o per la gestione dell'energia consumata o per la gestione ambientale dei propri Data Center. A tale riguardo, il soggetto può fare riferimento, rispettivamente, agli standard ISO 14064, ISO 50001 e ISO 14001, o equivalenti.*

RE.GE-02: Valutazione annuale dell'efficienza energetica del Data Center

1_O. *Il soggetto determina con frequenza annuale l'efficienza energetica dei propri Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5.*

Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura dei Data Center e quella sostenuta per gli apparati IT.

2.5 Sicurezza

IDENTIFY (ID)

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

ID.AM-01: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione

1_O. *Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.*

2_O. *Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.*

ID.AM-03: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati

1_O. *Tutti i flussi di dati e di informazioni, inclusi quelli verso l'esterno e relativi all'infrastruttura digitale, sono identificati, censiti e approvati da attori interni al soggetto.*

ID.AM-06: 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_O. *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_O. *È nominato, nell'ambito dell'articolazione di cui al punto 1_O., un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.*

3_O. *Sono nominati, nell'ambito dell'articolazione di cui al punto 1_O., 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 Italia ai fini della gestione degli incidenti aventi impatto sull'Infrastruttura digitale.*

4_O. *L'incaricato di cui al punto 2_O. e il referente tecnico di cui al punto 3_O. operano in stretto raccordo.*

2.5.2) 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.

ID.GV-01: È identificata e resa nota una policy di cybersecurity

1_O. *Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.*

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

ID.RA-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

- ***1_O.*** *Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dell'Infrastruttura digitale e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione.*
- ***2_O.*** *Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).*

ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio

- ***1_O.*** *L'analisi del rischio è svolta 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_O.*** *L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale.*
- ***3_O.*** *Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.*

PROTECT (PR)

2.5.4) Identity Management, Authentication and Access Control (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.

PR.AC-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

- ***1_O.a*** *Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.*
- ***1_O.b*** *Le credenziali di accesso sono individuali per il personale del soggetto e per il personale esterno che ha accesso all'infrastruttura e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.*
- ***2_O.*** *Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1_O., le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.*
- ***3_O.*** *Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.*
- ***4_O.*** *Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es. trasferimento di personale).*
- ***5_O.*** *Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.*
- ***6_O.*** *Esiste una pianificazione aggiornata degli audit di sicurezza per verificare il rispetto di quanto previsto nei punti 1_O., 2_O., 3_O., 4_O. e 5_O. ed esiste un registro degli audit effettuati con la relativa documentazione.*

PR.AC-02: L'accesso fisico alle risorse è protetto e amministrato

- ***1_O.*** *Con riferimento ai censimenti della sottocategoria ID.AM-01, 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.

2_O. *È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi.*

PR.AC-03: L'accesso remoto alle risorse è amministrato

1_O. *Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.*

2_O. *Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.*

3_O. *È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.*

4_O. *Esiste un log degli accessi eseguiti da remoto.*

5_O. *Per gli accessi da remoto, sono impiegati modalità di autenticazione a fattore multiplo.*

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

1_O. *Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno:*

a. le risorse censite a cui è necessario accedere, 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 a gruppi di utenti.

2_O. *Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.*

3_O. *Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.*

2.5.5) Awareness and Training (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.

PR.AT-01: Il personale del soggetto è informato e addestrato

1_O. *Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti.*

2_O. *L'addestramento e la formazione di cui al punto 1_O. fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche:*

a. la tutela della confidenzialità di dati in chiaro o cifrati;

b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro;

c. la definizione di ruoli e delle responsabilità;

d. politiche di accesso a sistemi, asset e risorse;

e. politiche di gestione delle informazioni e della sicurezza;

f. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;

g. requisiti per la non divulgazione/confidenzialità di informazioni.

PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

1_O. *Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.*

2_O. *Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.*

2.5.6) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

1_O. *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.

2_O. *I dati dell'amministrazione, ivi inclusi quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Salvo motivate e documentate ragioni di natura normativa o tecnica, nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di:*

a. Business Continuity e Disaster Recovery, anche se esternalizzate (ad esempio tramite cloud computing);

b. Content Delivery Network con distribuzione geografica globale.

In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali.

3_O. *Diversamente dal caso dei Metadata relativi al funzionamento dell'infrastruttura, che possono essere trattati mediante infrastrutture localizzate anche al di fuori del territorio dell'Unione europea, i Metadata relativi all'amministrazione sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di Metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.*

4_O. *Con riferimento al punto 3_O., nel caso in cui i Metadata relativi all'amministrazione siano finalizzati all'erogazione di servizi per la sicurezza informatica ovvero per la resilienza dell'infrastruttura digitale, essi possono essere trattati, in presenza di motivate ragioni tecniche e relative evidenze di una loro gestione conforme all'univocità delle finalità del trattamento, anche fuori del territorio europeo. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.*

PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)

1_O. *Sono definite 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.

2_O. *Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.*

PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

1_O. *Sono definiti 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.

2.5.7) Information Protection Processes and Procedures (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.

PR.IP-01: 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_O. *Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale.*

PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati

1_Oa. *Viene effettuato periodicamente un backup dei dati memorizzati. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup.*

1_Ob. *Viene effettuato periodicamente un backup delle informazioni memorizzate nel cloud necessarie per il completo ripristino del sistema, ivi incluso i dati dell'Amministrazione e i dati necessari per il ripristino del servizio. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup. A tal fine, viene anche assicurato che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.*

2_O. *Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come obiettivo (SLO) almeno 1 volta all'anno.*

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

1_O. *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.

2_O. *Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, della threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale.*

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

PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

1_O. *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-03 e dei seguenti punti.*

2_O. *Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.*

2.5.9) Protective Technology (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.

PR.PT-04: Le reti di comunicazione e controllo sono protette

1_O. *I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati.*

DETECT (DE)

2.5.10) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

DE.CM-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

- ***1_O.*** *Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS).*
- ***2_O.*** *Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.*

DE.CM-04: Il codice malevolo viene rilevato

- ***1_O.*** *Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection System - EPS).*
- ***2_O.*** *Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.*

DE.CM-08: Vengono svolte scansioni per l'identificazione di vulnerabilità

- ***1_O.*** *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_O.*** *Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software, di cui al punto 1_O.*
- ***3_O.*** *Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.*
- ***4_O.*** *Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.*

2.5.11) Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.

DE.DP-01: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability

- ***1_O.*** *Le nomine di cui alla sottocategoria ID.AM-06 sono rese note all'interno del soggetto.*
- ***2_O.*** *I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.*

RESPOND (RS)

2.5.12) Communications (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).

RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

- ***1_O.*** *I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di risposta ad un incidente sono ben definiti e resi noti alle articolazioni competenti del soggetto.*

2.5.13) Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace risposta e supporto alle attività di ripristino.

RS.AN-05: 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_O.*** *I canali di comunicazione del CSIRT Italia 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 (ISAC) di riferimento sono monitorati.*

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

RS.MI-03: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

1_O. *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.*

2_O. *Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.*

RECOVER (RC)

2.5.15) Recovery Planning (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.

RC.RP-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity

1_O. *Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.*

3. Livelli minimi previsti nel caso di dati e servizi critici

3.1 Affidabilità

3.1.1) Business Continuity e Disaster Recovery.

A.BC-01: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti

3_C. *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui requisito A.BC-01, punto 2_O. In particolare, con riferimento al requisito A.BC-01, punto 1_O., l'infrastruttura digitale è dotata di soluzioni di DR, con caratteristiche coerenti con l'analisi del rischio, e devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 36 ore e RPO 36 ore.*

3.1.2) Governance e processi.

A.GP-02: È garantito il rispetto degli indicatori di servizio obbligatori

3_C. *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui al punto 2_O. Il servizio di supporto e assistenza è fornito, almeno in lingua italiana, tutti i giorni dell'anno a qualsiasi orario (24 ore al giorno, 7 giorni a settimana per tutto l'anno).*

3.1.3) Performance e Scalabilità.

A.PS-01: Sono garantite caratteristiche minime di connettività

2_C. *Il soggetto offre meccanismi di protezione contro eventi cyber di tipo Denial-of-Service / Distributed Denial-of-Service.*

3.2 Data Center Security

3.2.1) Data Center Security.

S.DC-03: La progettazione/realizzazione del Data Center garantisce la manutenibilità a caldo, conformemente agli standard di mercato

1_C. *L'infrastruttura digitale deve aderire ai parametri del certificato ANSI/TIA 942B con rating "Concurrent Maintainability" oppure a quello di Tier III dell'Uptime Institute. In alternativa deve essere conforme alle caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio riportati alla Tabella 1.*

3.3 Sicurezza

IDENTIFY (ID)

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

ID.AM-02: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione

- ***1_C.*** *Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.*
- ***2_C.*** *L'installazione delle piattaforme e delle applicazioni software è consentita esclusivamente per quelle approvate.*
- ***3_C.*** *Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione.*

ID.AM-06: 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)

- ***5_C.*** *I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2_O. e del referente tecnico di cui al punto 3_O. sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).*
- ***6_C.*** *Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.*
- ***7_C.*** *Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2_O. e al referente tecnico di cui al punto 3_O. presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.*
- ***8_C.*** *L'incaricato di cui al punto 2_O. assicura, inoltre, la collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge n. 105 del 2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge n. 82 del 2021, e alle attività di verifica e ispezione.*

3.3.2) 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.

ID.GV-01: È identificata e resa nota una policy di cybersecurity

- ***2_C.*** *Il documento di cui al punto 1_O. deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.*

ID.GV-04: La governance ed i processi di risk managament includono la gestione dei rischi legati alla cybersecurity

- ***1_C.*** *Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy dell'Infrastruttura.*

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

ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio

- ***4_C.*** *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 alla sottocategoria DE.CM-8;*
  - *c. i potenziali impatti ritenuti significativi sull'infrastruttura, opportunamente descritti e valutati;*
  - *d. l'identificazione, l'analisi e la ponderazione del rischio.*

3.3.4) Supply Chain Risk Management (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.

ID.SC-01: 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_C.*** *Esiste un documento aggiornato di dettaglio che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber.*
- ***2_C.*** *Tali processi sono validati e approvati da parte dei vertici del soggetto.*

PROTECT (PR)

3.3.5) Identity Management, Authentication and Access Control (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.

PR.AC-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

- ***7_C.*** *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 le procedure di cui ai punti 1_O., 2_O., 3_O., 4_O., 5_O., 6_O.;*
  - *b. 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;*
  - *c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.*

PR.AC-02: L'accesso fisico alle risorse è protetto e amministrato

- ***3_C.*** *È definito un perimetro di sicurezza tra le aree amministrative e le aree di data storage e processing.*

PR.AC-03: L'accesso remoto alle risorse è amministrato

- ***6_C.*** *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. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.*

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

- ***4_C.*** *Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1_O..*

PR.AC-05: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

- ***1_C.*** *Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.*
- ***2_C.*** *È definito un piano per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste.*

PR.AC-07: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, 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_C.*** *Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.*

3.3.6) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

5_C. *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui punto 4_0. Con riferimento al trattamento dei Metadati relativi all'amministrazione, resta fermo, pertanto, quanto previsto dal punto 3_O..*

PR.DS-02: I dati sono protetti durante la trasmissione

1_C. *Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.*

2_C. *Conformemente all'analisi del rischio di cui alla misura ID.RA-05, per i flussi di dati e le comunicazioni di cui alla misura ID.AM-03 sono utilizzati canali di comunicazione sicuri e criptati e protocolli aggiornati e approvati.*

PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

1_C. *Sono definite 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.

PR.DS-07: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

1_C. *Sono definite 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.

3.3.7) Information Protection Processes and Procedures (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.

PR.IP-03: Sono attivi processi di controllo della modifica delle configurazioni

1_C. *Sono definite:*

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.

2_C. *È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.*

3_C. *Sono definiti e implementati i piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.*

PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati

3_C. *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.

PR.IP-09: 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_C.*** *Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi l'infrastruttura digitale.*
- ***2_C.*** *Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta 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 Italia.
- ***3_C.*** *Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.*
- ***4_C.*** *I piani di business continuity sono collaudati e comunicati alle parti interessate.*
- ***5_C.*** *La documentazione di cui al punto 2_C. è resa disponibile, ove richiesto, all'Amministrazione ed è rivista periodicamente.*
- ***6_C.*** *L'impatto derivante da interruzione ed eventuali rischi è determinato al fine di stabilire criteri per sviluppare strategie e capacità di business continuity.*

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

PR.MA-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

- ***1_C.*** *Sono definite in relazione alla categoria ID.AM:*
  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.

PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

- ***3_C.*** *Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.*
- ***4_C.*** *Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.*
- ***5_C.*** *Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.*

3.3.9) Protective Technology (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.

PR.PT-01: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

- ***1_C.*** *I log son conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi*
- ***2_C.*** *Sono definite:*
  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.

PR.PT-04: Le reti di comunicazione e controllo sono protette

- ***2_C.*** *Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.*
- ***3_C.*** *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.*

PR.PT-05: 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_C. *In relazione ai piani previsti dalla sottocategoria PR.IP-09:*
a. sono adottate architettura ridondate di rete, di connettività, nonché applicative.

2_C. *Esistono meccanismi per garantire la continuità operativa, nel rispetto delle misure di sicurezza qui elencate.*

3_C. *Sono definite:*
a. le politiche di sicurezza adottate in relazione ai punti 1_C. e 2_C.;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DETECT (DE)

3.3.10) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

1_C. *Ai fini di rilevare tempestivamente incidenti con impatto sull'Infrastruttura digitale, sono adottati gli strumenti tecnici e procedurali per:*
a. acquisire le informazioni da più sensori e sorgenti;
b. ricevere e raccogliere informazioni inerenti alla sicurezza dell'Infrastruttura digitale rese note dal CSIRT Italia, da fonti interne o esterne al soggetto;
c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a) e b), per rilevare tempestivamente eventi di interesse.

2_C. *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_C. *Sono definite:*
a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1_C., lettera a);
b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1_C., lettere a) e b);
c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1_C., lettera c);
d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2_C..

4_C. *Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.*

5_C. *È adottato un sistema di auditing per le attività relative al rilevamento di informazioni inerenti alla sicurezza, al monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o Metadati.*

6_C. *Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile.*

3.3.11) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

DE.CM-07: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

1_C. *Con riferimento alla sottocategoria PR.AC-03, 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_C. *Con riferimento alla sottocategoria ID.AM-01, 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_C. *Gli strumenti tecnici di cui ai punti 1_C. e 2_C. 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_C. *Esiste un documento aggiornato che descrive, almeno:*
a. le politiche di sicurezza adottate in relazione ai punti 1_C. e 2_C.;

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

3.3.12) Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.

DE.DP-01: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability

- ***1_C.*** *Le nomine di cui alla sottocategoria ID.AM-06 sono rese note all'interno del soggetto.*
- ***2_C.*** *I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.*
- ***3_C.*** *Esiste un documento aggiornato di dettaglio che indica almeno:*
  a. i ruoli, i processi e le responsabilità di cui al punto 2_O.;
  b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1_O. e 2_O..
- ***4_C.*** *È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate.*

RESPOND (RS)

3.3.13) Response Planning (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

RS.RP-01: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente

- ***1_C.*** *Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DETECT (DE) nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sull'infrastruttura digitale.*

3.3.14) Communications (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).

RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

- ***1_C.*** *I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di risposta ad un incidente sono ben definiti e resi noti alle articolazioni competenti del soggetto.*
- ***2_C.*** *Sono eseguite periodicamente esercitazioni.*
- ***3_C.*** *Esiste un documento aggiornato di dettaglio che indica almeno:*
  a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1_O. e 2_C.;
  b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1_O. e _C.2;
  c. le modalità per le esercitazioni di cui al punto 3.
- ***4_C.*** *Il soggetto provvede a notificare l'Amministrazione di un incidente o data breach entro 1 ora dalla registrazione e classificazione dell'evento.*
- ***5_C.*** *Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale.*

RS.CO-05: E' attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awarenesss)

- ***1_C.*** *Sono definiti e mantenuti contatti con gruppi di interesse legati all'Infrastruttura digitale e alla cyber sicurezza, nonché con altre entità rilevanti in linea con il contesto del soggetto in relazione all'Infrastruttura digitale.*
- ***2_C.*** *Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.*

3.3.15) Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace risposta e supporto alle attività di ripristino.

RS.AN-05: 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_C. *I canali di comunicazione del CSIRT Italia 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 (ISAC) di riferimento sono monitorati.*

2_C. *Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-03 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-08 sono diffusi alle articolazioni competenti del soggetto.*

3_C. *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_O. e 2_O.;

b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1_O. e 2_O..

RECOVER (RC)

3.3.16) Recovery Planning (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.

RC.RP-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity

2_C. *Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.*

4. Livelli minimi previsti nel caso di dati e servizi strategici

4.1 Affidabilità

4.1.1) Business Continuity e Disaster Recovery.

A.BC-01: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti

4_S. *Nel caso di dati e di servizi strategici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui requisito A.BC-01, punto 3_O. In particolare, con riferimento al requisito A.BC-01, punto 1_O., l'infrastruttura digitale è dotata di soluzioni di DR, con caratteristiche coerenti con l'analisi del rischio, e devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 24 ore e RPO 24 ore.*

4.2 Sicurezza

IDENTIFY (ID)

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

ID.AM-06: 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)

5_S. *I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2_O. e del referente tecnico di cui al punto 3_O. sono comunicati dal soggetto all'Agenzia per la cybersicurezza nazionale (ACN).*

4.2.2) 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.

ID.GV-01: È identificata e resa nota una policy di cybersecurity

- ***3_S.*** *Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1_O. deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato.*
- ***4_S.*** *Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti.*

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

ID.RA-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

- ***3_S.*** *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.
- ***4_S.*** *Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.*

4.2.4) Supply Chain Risk Management (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.

ID.SC-01: 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

- ***3_S.*** *All'interno dell'organizzazione, sono presenti ed aggiornate almeno su base annuale le politiche e le procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa rispetto a soggetti esterni e/o Amministrazioni terze (Shared Security Responsibility Model-SSRM).*
- ***4_S.*** *Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi incluse le Infrastrutture digitali.*

ID.SC-02: 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_S.*** *In merito all'affidamento di forniture 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-06, punto 2_O., 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 dell'Infrastruttura digitale;
  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_S. *Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura dell'Infrastruttura digitale, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1_S. lettera d..*

3_S. *Si raccomanda, ove possibile e in relazione alla criticità di:*

a. valutare l'affidabilità tecnica di cui al punto 1_S., 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 ed eseguito,

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.

ID.SC-03: 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_S. *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 all'infrastruttura digitale. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.*

2_S. *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 all'infrastruttura digitale. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.*

ID.SC-04: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1_S. *Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.*

2_S. *Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.*

3_S. *È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio.*

4_S. *Le politiche e le procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno su base annuale.*

5_S. *È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation, relativo alle le azioni correttive connesse alle non conformità rilevate sui fornitori e partner terzi.*

PROTECT (PR)

4.2.5) Identity Management, Authentication and Access Control (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.

PR.AC-03: L'accesso remoto alle risorse è amministrato

7_S. *Le politiche e le procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, del soggetto.*

8_S. *È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati dello stesso. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati.*

9_S. *Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate.*

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

5_S. *Il soggetto è autonomo nella gestione dell'infrastruttura, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.*

PR.AC-05: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

3_S. *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 use sono limitati e/o monitorati.

PR.AC-07: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, 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)

2_S. *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.

4.2.6) Awareness and Training (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.

PR.AT-01: Il personale del soggetto è informato e addestrato

3_S. *Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.*

PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

3_S. *Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1_O. e 2_O..*

4.2.7) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

6_S. *Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto:*

a. segnala all'Agenzia per la cybersicurezza nazionale (ACN) e all'amministrazione ogni richiesta di accesso a dati o Metadati da parte di entità extra-UE;

b. fornisce accesso a dati dell'amministrazione o Metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'amministrazione.

7_S. *Sono definite ed implementate procedure e misure tecniche per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi.*

8_S. *Nel caso di dati e di servizi strategici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui punto 3_O.. Al riguardo, tutte le tipologie di metadata devono essere trattate mediante infrastrutture localizzate sul territorio dell'Unione europea, ad eccezione di quelli necessari all'erogazione dei servizi indicati al punto 2_O..*

PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

2_S. *Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti che, qualora compromessi, possano avere impatti sulla disponibilità, integrità o confidenzialità dell'infrastruttura o dei servizi erogati dalla stessa.*

3_S. *Coerentemente con quanto previsto dal punto 2_S., sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto.*

4_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_C..*

PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)

3_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

2_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

PR.DS-07: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

2_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_C..*

4.2.8) Information Protection Processes and Procedures (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.

PR.IP-01: 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)

2_S. *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 il dispiegamento delle sole configurazioni adottate;

b. l'elenco delle configurazioni dei sistemi IT e 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_S. *Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.*

4_S. *Sono definite ed implementate metriche, di natura tecnica, utili a monitorare il livello di aderenza ai requisiti di sicurezza definiti e gli obblighi di conformità.*

5_S. *Esiste un processo di mitigazione delle vulnerabilità applicative e ripristino per la sicurezza delle applicazioni, automatizzando la riparazione quando possibile.*

6_S. *È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni.*

7_S. *È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni.*

PR.IP-03: Sono attivi processi di controllo della modifica delle configurazioni

4_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_C..*

PR.IP-09: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro

- ***7_S.*** *Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dall'Infrastruttura digitale e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery.*
- ***8_S.*** *Esiste un documento aggiornato di dettaglio contenente i piani di 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 Italia.
- ***9_S.*** *Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.*
- ***10_S.*** *Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate.*
- ***11_S.*** *I dispositivi critici per il funzionamento dell'infrastruttura sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore.*

PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)

- ***1_S.*** *Il soggetto rende disponibile all'amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura o ai dati dell'amministrazione.*
- ***2_S.*** *Il soggetto rende disponibile all'amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'amministrazione. L'amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il soggetto provvede nel senso tempestivamente.*

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

- ***3_S.*** *Il documento di cui al punto 1_O. dovrà essere aggiornato su base semestrale.*
- ***4_S.*** *Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management.*

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

PR.MA-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

- ***2_S.*** *Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.*
- ***3_S.*** *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_C..*
- ***4_S.*** *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.*
- ***5_S.*** *In base all'analisi del rischio di cui alla misura ID.RA-05, ogni aggiornamento hardware o software di componenti 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, se del caso, il relativo codice oggetto dovrà essere custodito per almeno 24 mesi. Le attività in ambiente di test sono volte a verificare anche aspetti di sicurezza.*
- ***6_S.*** *Gli aggiornamenti software devono essere consentiti solo da fonti pre-autorizzate.*
- ***7_S.*** *Tutti i log relativi alle attività di manutenzione e aggiornamento dovranno essere prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività.*
- ***8_S.*** *Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 5_S., 6_S. e 7_S..*

PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

6_S. *Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2_O., 3_C., 4_C. e 5_C..*

4.2.10) Protective Technology (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.

PR.PT-01: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

3_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_C..*

PR.PT-04: Le reti di comunicazione e controllo sono protette

1_S. *I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati.*

2_S. *Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.*

3_S. *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.*

4_S. *L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1_O. e 2_C. sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA.*

5_S. *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. sono impiegati anche per i fini di cui alla funzione DETECT (DE).*

6_S. *Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1_O., 2_C., 3_C., 4_S e 5_S..*

PR.PT-05: 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

4_S. *In relazione ai piani previsti dalla sottocategoria PR.IP-09:*
a. esiste un sito di disaster recovery, con caratteristiche coerenti con l'analisi del rischio.

5_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui ai punti 1_C., 2_C., 3_C. e 4_S..*

DETECT (DE)

4.2.11) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

7_S. *Esiste un repository centralizzato che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto.*

8_S. *Esiste un documento aggiornato di dettaglio, recante i processi e le politiche di cui al punto 3_C..*

4.2.12) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

DE.CM-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

3_S. *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.*

4_S. *Gli strumenti tecnici di cui ai punti 1_O. e 3_S. sono aggiornati, manutenuti 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.*

5_S. *Gli strumenti tecnici di cui al punto 1_O. sono impiegati anche per i fini di cui alla categoria DE.AE.*

6_S. *Esiste un documento aggiornato che descrive, almeno:*
a. le politiche di sicurezza adottate in relazione al punto 2_O.;

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

DE.CM-04: Il codice malevolo viene rilevato

- ***3_S.*** *Sono configurati appositi software firewall su tutti i dispositivi.*
- ***4_S.*** *I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox.*
- ***5_S.*** *Gli strumenti tecnici di cui ai punti 1_O., 3_S. e 4_S. 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_S.*** *Esiste un documento aggiornato che descrive, almeno:*
  a. le politiche di sicurezza adottate in relazione ai punti 1_O., 2_O., 3_S. e 4_S.;
  b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DE.CM-07: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

- ***5_S.*** *Con riferimento alla sottocategoria ID.AM-02, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.*
- ***6_S.*** *Con riferimento alla sottocategoria ID.AM-03, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.*
- ***7_S.*** *Gli strumenti tecnici di cui ai punti 5_S. e 6_S. 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.*
- ***8_S.*** *Esiste un documento aggiornato che descrive, almeno:*
  a. le politiche di sicurezza adottate in relazione ai punti 5_S. e 6_S.;
  b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

RESPOND (RS)

4.2.13) Response Planning (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

RS.RP-01: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente

- ***2_S.*** *Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.*
- ***3_S.*** *Il piano di risposta e le politiche e procedure di cui ai punti 1_C. e 2_S. includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.*
- ***4_S.*** *I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi.*
- ***5_S.*** *Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity.*
- ***6_S.*** *Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.*
- ***7_S.*** *Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.*

4.2.14) Communications (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).

RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

- ***5_S.*** *Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale.*
- ***6_S.*** *Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned).*
- ***7_S.*** *Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.*
- ***8_S.*** *È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili.*
- ***9_S.*** *Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione.*
  In particolare, 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 interlocuzione con il CSIRT Italia.

RECOVER (RC)

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

RC.IM-02: Le strategie di recupero sono aggiornate

- ***1_S.*** *Il piano di cui alla sottocategoria RC.RP-01 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.*

4.2.16) Communications (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).

RC.CO-03: 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_S.*** *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).*

5. Livelli minimi con termini di adozione differiti

5.1. Si riporta di seguito l'elenco dei requisiti da rispettare decorsi sei mesi dalla data di applicazione del presente Regolamento, aggiuntivi rispetto a quelli immediatamente applicabili alla data di entrata in vigore:

- A.PS-01.2_C.
- DE.DP-01.1_O.
- DE.DP-01.2_O.
- ID.AM-06.5_C.
- PR.IP-04.1_Ob.
- PR.DS-02.2_C.
- PR.AC-01.1_O.b
- PR.AC-03.5_O.
- PR.PT-04.1_O.
- PR.PT-04.2_C.
- PR.PT-04.3_C.
- RS.AN-05.1_O.

- RS.CO-01.1_O.
- RS.CO-01.5_C..

6. Appendice

Tabella 1: Caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio

Best practices ANSI/TIA492, Normativa anti-incendio nazionale

Topic	***Caratteristica***
Misure di protezione contro minacce di incendio e fumo	*Sono implementate misure di protezione contro minacce di incendio e fumo.*
Sorveglianza dei parametri operativi e ambientali	*I servizi di utility del Data Center e le condizioni ambientali (acqua, elettricità, controlli di temperatura e umidità, telecomunicazioni e connettività) sono protetti, monitorati, manutenuti e testati per l'efficacia continua a intervalli pianificati per garantire la protezione da eventi non autorizzati. Qualora i valori di benchmark dei parametri operativi delle utility e ambientali venga superato, devono essere avviate tempestivamente le misure necessarie per il ripristino al range di controllo.*
Sistema di raffreddamento	*Il soggetto deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.*
Ridondanza sistema di connettività	*Il Data Center dispone di un sistema di connettività di rete ridondato tramite l'utilizzo di almeno due distinti carrier in ingresso (connettività multi-carrier).*
Sito Geografico, prossimità corsi d'acqua	*La distanza del CED dai corsi d'acqua è maggiore di 91 m.*
Sito Geografico, prossimità arterie autostradali/ferroviarie	*La distanza del CED da arterie autostradali e ferroviarie è maggiore di 91 m.*
Sito Geografico, prossimità aeroporti	*La distanza del CED dagli aeroporti è maggiore di 1,6 km.*
Prossimità del parcheggio visitatori ai muri perimetrali del Data Center	*Il parcheggio visitatori dispone di barriere di protezione per impedire la collisione di veicoli con il muro esterno di facility e computer room, distante almeno 9,1 m.*
Parcheggio dipendenti separato dal parcheggio visitatori	*ll parcheggio visitatori è separato fisicamente da quello dei dipendenti da una recinzione o da un muro e deve avere ingresso separato.*
Area carico/scarico separata dal parcheggio	*L'area carico/scarico è separata fisicamente dal parcheggio mediante una recinzione o un muro con ingressi separati, o con un sistema con controllo accesso fisico, in modo da eliminare le interferenze fra le operazioni di carico/ scarico e il passaggio di auto.*
Cablaggi telecomunicazioni e percorsi orizzontali ridondanti	*I cablaggi di telecomunicazione e i percorsi orizzontali sono ridondati.*
Pozzetti di Accesso della fibra	*I pozzetti di accesso della fibra hanno una distanza superiore ai 20 m.*
Ridondanza area dedicata all'attestazione della fibra con gli apparati dei carrier/provider	*L'area dedicata all'attestazione della fibra con gli apparati dei carrier/provider provenienti dai pozzetti di ingresso è ridondata con la logica di collegamento diretto e incrociato.*
Router e Switch hanno alimentatori e control station ridondati	*Gli apparati router e switch possiedono alimentatori e control station ridondati.*
Router ridondanti e switch con uplink ridondato	*Gli apparati router e switch possiedono uplink ridondato.*
Separazione antincendio corridoi sala computer e aree di supporto	*I corridoi di uscita dalla sala computer e dalle aree di supporto sono separati con soluzioni antincendio con almeno resistenza REI 60.*
Larghezza dei corridoi di uscita	*La larghezza dei corridoi di uscita non è inferiore a 1,2 m.*
Area spedizioni separata fisicamente dalle altre aree del Data Center	*L'area spedizioni è separata fisicamente dalle altre aree del Data Center.*
Numero di banchine di carico in area di spedizione/ricezione	*È presente almeno una banchina di carico in area di spedizione/ricezione.*
Prossimità locali di stoccaggio combustibile e generatori	*I locali di stoccaggio combustibile e generatori alle sale dati ed alle aree di supporto sono separati dalle sale dati e dalle aree di supporto con una compartimentazione almeno REI 120. Se all'esterno, sono rispettate le prescrizioni dei Vigili del Fuoco.*

Sistema di controllo, dispositivi in campo e apparati di visualizzazione sotto continuità	*Per il Sistema di controllo (TVCC, Accessi, Antiintrusione), i dispositivi in campo e gli apparati di visualizzazione è garantita la continuità con UPS dedicato al sistema di controllo e visualizzazione oppure tramite batterie locali sui dispositivi di campo, con autonomia di 8 ore.*
Personale di sicurezza fisica	*Il presidio di sicurezza fisica è 24h/gg.*
Controllo accessi ai varchi di tutte le sale del Data center	*Il controllo degli accessi ai varchi di tutte le sale del Data Center, compresa l'entrata principale, è effettuato con badge o biometrico, deve essere presente un sistema antiintrusione, un allarme porta/ finestra aperta.*
Misure protettive per rack /armadi di apparecchiature per telecomunicazione	*I Rack / armadi di apparecchiature per telecomunicazioni sono fissati alla base o supportati in alto e alla base o sono dotati di piattaforme sismiche o di altre misure protettive.*
Ingresso dell'edificio con guardiola e bancone della sorveglianza	*All'ingresso all'edificio sono presenti una guardiola ed un bancone di sorveglianza per il controllo dei documenti e delle autorizzazioni, adeguatamente protetto (requisito di vetro antiproiettile livello 3).*
Ingresso dell'edificio con porte e finestre antincendio	*L'ingresso dell'edificio è protetto con porte e finestre antincendio almeno REI 60. È considerato conforme un permesso specifico rilasciato dai Vigili del Fuoco.*
Protezione Ingresso edificio	*L'ingresso all'edificio è protetto con porte interbloccate con accesso singolo, sistemi fisici anti-scavalcamento e anti-passback.*
Uffici amministrativi separati dall'area del CED	*Gli uffici amministrativi sono separati dall'area del Data Center.*
Prossimità di servizi igienici o sale ristoro alle sale dati	*I servizi igienici o le sale ristoro adiacenti al Data Center dispongono di un sistema antiallagamento.*
Separazione antincendio dei servizi igienici e sale ristoro dalle sale dati e dalle aree di supporto	*I servizi igienici e le sale ristoro adiacenti al Data Center sono separati con sistemi antincendio resistenti almeno REI 60.*
Controllo TVCC a tutte le aree ristrette con accesso tramite porte con badge	*Tutte le aree ristrette con accesso tramite porte con badge sono controllate con sistemi TVCC.*
TVCC dei varchi con controllo d'accesso	*I varchi di controllo di accesso sono controllati con sistemi TVCC.*
Registrazione TVCC di tutte le attività su tutte le telecamere	*Il periodo di retention delle registrazioni TVCC è almeno di 30 giorni.*
Frequenza immagini TVCC (frame rate)	*La frequenza delle immagini TVCC è almeno pari a 20 frame/sec.*
Il sistema di distribuzione elettrica consente la manutenzione a caldo	*Il sistema di distribuzione elettrica consente la manutenzione a caldo senza esclusioni.*
Analisi del sistema elettrico	*Il sistema elettrico è stato sottoposto ad analisi corredata da una relazione di progetto che deve comprendere il calcolo delle potenze di corto circuito, studio di coordinamento verticale, analisi dell'arco elettrico e studio del flusso di carico.*
Cavi elettrici per computer e apparecchiature per telecomunicazioni	*I cavi elettrici per computer e apparecchiature per telecomunicazioni sono ridondanti con capacità del 100% sui rimanenti cavo o cavi.*
Ridondanza sistemi UPS	*La ridondanza dei sistemi UPS è N+1.*
Bypass automatico e bypass di manutenzione	*Sono stati adottati un bypass automatico alimentato con interruttore dedicato e un interruttore di bypass esterno per esclusione totale UPS.*
Distribuzione elettrica in uscita dai sistemi UPS	*Il quadro elettrico relativo alla distribuzione elettrica in uscita dagli UPS ha interruttori estraibili con funzioni adjustable long time e instantaneous trip.*
Tipo di batterie dei sistemi UPS	*Le batterie sono state progettate per 5-10 anni di vita media con UPS statici oppure UPS rotanti.*
Durata minima delle batterie dei sistemi UPS	*La durata minima delle batterie è di 10 minuti con UPS statici o UPS rotanti.*
Sistema di monitoraggio delle batterie dei sistemi UPS	*Il sistema di monitoraggio delle batterie è gestito dall'UPS a livello dei banchi delle batterie.*
Topologia sistemi UPS	*Gli UPS sono ridondati e distribuiti su moduli o blocchi.*
Procedura di bypass per manutenzione del commutatore statico	*La procedura di bypass per la manutenzione del commutatore è manuale guidata con dispositivo di blocco meccanico.*

Trasformatore	*Il trasformatore è di tipo K-Rated / Harmonic Canceling, (o tecnologia equivalente) ad efficienza elevata.*
Impianto di protezione dalle scariche atmosferiche	*È stato adottato un impianto di protezione dalle scariche atmosferiche.*
Messa a terra delle masse metalliche in Computer Room	*Le masse metalliche in Computer Room dispongono di impianto di messa a terra.*
Punti monitorati	*I punti monitorati sono almeno la rete elettrica pubblica, il trasformatore principale, l'UPS, il generatore, lo stato degli interruttori, i Static Transfer Switch e l'Automatic Transfer Switch, le Power Distribution Unit.*
Metodo di notifica degli allarmi	*Il metodo di notifica degli allarmi innescati dal monitoraggio avviene presso la sala di controllo, tramite cercapersone, e-mail e/o SMS.*
Locale batterie separato dal locale UPS	*Il locale batterie non è separato del locale UPS a meno che non sia richiesto dai VVFF. La separazione è preferibile.*
Gruppi di batterie isolati	*I singoli gruppi di batterie sono isolati fra loro.*
Dimensionamento dei generatori elettrici automatici di backup (Standby generating system)	*I generatori elettrici automatici di backup sono dimensionai per il carico dell'intero edificio e con ridondanza N+1*
Generatori su singola barratura	*I generatori elettrici hanno la barratura di potenza opportunamente dimensionata.*
Disponibilità Load bank	*È disponibile un load bank portatile (di proprietà o in affitto).*
Esecuzione test di accettazione in fabbrica (FAT) apparati elettrici	*Gli UPS ed i generatori sono stati sottoposti a test di accettazione in fabbrica (FTA).*
Procedura di collaudo in produzione apparati elettrici	*Gli apparati elettrici sono stati collaudati in produzione a livello di componenti e di sistema tramite opportuna procedura.*
Personale operativo e di manutenzione apparati elettrici	*Il Personale operativo e di manutenzione degli apparati elettrici è presente on site 24 ore su 7 giorni.*
Manutenzione preventiva apparati elettrici	*Il generatore e gli UPS sono sottoposti a manutenzione preventiva.*
Programma di formazione del personale operativo	*È stato definito un programma di formazione del personale operativo rispetto al regolare esercizio degli apparati.*
Ridondanza degli apparati meccanici	*Gli apparati meccanici (es. unità di condizionamento, dry cooler, pompe, torri evaporative, condensatori) hanno una ridondanza pari a N+1, allo scopo di garantire le operazioni di manutenzione a caldo. Le caratteristiche di ridondanza si applicano anche alle aree di supporto che non sono critiche alla continuità delle operazioni della computer room. Le manovre per garantire la manutenzione a caldo possono essere manuali.*
Passaggio di tubazioni non attinenti al data center all'interno dello spazio data center	*Non è permesso che ci sia un passaggio di tubazioni non attinenti al Data Center all'interno dello spazio della sala CED.*
Pressione dell'aria in Computer Room e nelle aree pertinenti	*La pressione all'interno della Computer Room e nelle aree pertinenti alla Computer Room è maggiore di quella delle altre aree.*
Pozzetti di scarico in Computer Room	*All'interno della Computer room sono presenti pozzetti di scarico per la condensa, per gli eventuali apparati di umidificazione e per l'impianto sprinkler, se presente.*
Alimentazione Sistemi meccanici	*I sistemi meccanici sono alimentati dal gruppo elettrogeno in mancanza di rete pubblica.*
Controllo dell'umidità nella Computer Room	*All'interno della Computer Room è monitorata l'umidità dell'aria.*
Unità interne sistemi di raffreddamento ad acqua	*Le unità interne dei sistemi raffreddati ad acqua sono ridondate (ogni 5-8 unità installate deve essere presente un'unità aggiuntiva).*
Alimentazione elettrica agli apparati meccanici	*L'alimentazione elettrica dei sistemi è ridondata (N+1) e configurata per garantire la manutenzione a caldo.*
Sistema di controllo HV AC	*Il sistema di controllo della ventilazione e del condizionamento dell'aria è progettato per garantire la manutenzione a caldo.*
Sistemi condensati ad acqua, Ripristino livello acqua dei circuiti	*Per i sistemi condensati ad acqua, il ripristino del livello di acqua nei circuiti deve avere due punti di connessione alla rete di alimentazione dell'acqua.*

Quantità di carburante per i generatori	*La quantità di carburante per i generatori garantisce un'autonomia di 48 ore (previo possesso di permesso specifico rilasciato dai Vigili del Fuoco).*
Serbatoi per Carburante per i generatori	*Sono presenti serbatoi multipli per il carburante per i generatori.*
Pompaggio carburante e tubazioni per i generatori	*Per ogni generatore è previsto il pompaggio del carburante e le tubazioni per i generatori.*
Impianto antincendio	*È presente un impianto Sprinkler per rilevazione e spegnimento dell'incendio nella parte uffici dell'edificio, o secondo le prescrizioni dei Vigili del Fuoco.*
Rilevazione Fumi VESDA per Computer Room ed Entrance Room con presenza di apparati attivi o sistema equivalente	*Nelle computer Room e nell'entrance room l'impianto antincendio è usata la tecnologia VESDA o un sistema equivalente per la rilevazione dei fumi.*
Spegnimento automatico a gas per Computer Room ed Entrance Room.	*Nelle computer Room e nell'entrance room è presente un impianto per lo spegnimento automatico a gas, con la presenza di apparati attivi.*
Sistema anti-allagamento per Computer Room ed Entrance Room con presenza di apparati attivi	*Nelle computer Room e nell'entrance room è presente un impianto antiallagamento, con la presenza di apparati attivi.*

REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, AI SENSI DELL'ARTICOLO 33-SEPTIES, COMMA 4, DEL DECRETO-LEGGE 18 OTTOBRE 2012, N. 179, CONVERTITO, CON MODIFICAZIONI, DALLA LEGGE 17 DICEMBRE 2012, N. 221

ALLEGATO 3

"CARATTERISTICHE DI BASE DI QUALITÀ, DI SICUREZZA, DI PERFORMANCE E DI SCALABILITÀ, DI INTEROPERABILITÀ, DI PORTABILITÀ DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE"

Sommario

1. **Premessa e definizioni** 1
2. **Caratteristiche di base previste nel caso di dati e servizi ordinari** 2
3. **Caratteristiche di base previste nel caso di dati e servizi critici** 15
4. **Caratteristiche di base previste nel caso di dati e servizi strategici** 23
5. **Caratteristiche di base con termini di applicazione differiti** 27

1. Premessa e definizioni

1.1. Il presente Allegato definisce, in conformità alle previsioni di cui all'articolo 6 del Regolamento le caratteristiche di base di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità dei servizi cloud per le pubbliche amministrazioni che possono ospitare, rispettivamente, servizi e dati digitali della pubblica amministrazione classificati, ai sensi del processo di cui all'articolo 5 del Regolamento, quali ordinari, critici o strategici.

1.2. Le caratteristiche di base sono organizzate sulla base delle sottocategorie del Framework Nazionale per la Cybersecurity e la Data Protection (di seguito FNCS) e definite tendendo conto della matrice CSA Cloud Control Matrix (CCM). 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.

1.3. Le caratteristiche di base di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità dei servizi cloud di cui al presente Allegato si applicano agli ambienti di produzione. le caratteristiche di base di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità degli ambienti di pre-produzione, test, sviluppo e ad essi assimilabili sono applicati in coerenza con le caratteristiche di base di cui al presente allegato, eventualmente in relazione ad un'analisi del rischio volta a individuare i potenziali impatti sul servizio e sui relativi dati gestiti ovvero sull'infrastruttura digitale relativa all'ambiente di produzione.

1.4. Ai fini del presente Allegato, si intende per:

a) "dati dell'amministrazione", dati forniti, conservati, inviati, ricevuti, trattati da o per conto dell'amministrazione dal soggetto tramite il servizio cloud;

b) "Metadata relativi all'Amministrazione", dati raccolti, ottenuti o generati dal soggetto, anche in forma derivata, a partire dai dati dell'amministrazione, nell'ambito dell'erogazione e dell'amministrazione del servizio cloud. In tale categoria rientrano, ad esempio la storicizzazione degli eventi dei sistemi e servizi, le configurazioni dei servizi e gli attributi delle risorse dell'amministrazione, derivanti anche dall'utilizzo degli stessi;

c) "Metadata relativi al funzionamento del Servizio Cloud", dati generati e utilizzati dal soggetto per monitorare e garantire la funzionalità del Servizio cloud, non inclusi in Metadata dell'amministrazione o dati dell'amministrazione. In tale categoria di Metadata, che non devono quindi essere riconducibili a persone, al soggetto e non possono comunque permettere

di estrarre - anche in parte - i dati dell'amministrazione, rientrano, ad esempio le metriche sulle performance d'utilizzo, bilanciamento, etc.

d) "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 dipende il funzionamento dell'infrastruttura digitale;
e) "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 servizio cloud, ma di pertinenza del fornitore di servizi cloud, da cui dipende il funzionamento dell'infrastruttura digitale;
f) "catena di approvvigionamento cyber", la catena di approvvigionamento relativa all'infrastruttura digitale.

1.5. Ad eccezione dell'organizzazione di cybersecurity, il termine "organizzazione", che compare all'interno delle descrizioni delle categorie e sottocategorie, è da intendersi riferito almeno all'infrastruttura o al personale del fornitore di servizi cloud preposto alla sua gestione. In aggiunta, il termine "soggetto" è da intendersi nell'accezione di "fornitore di servizi cloud".

2. Caratteristiche di base previste nel caso di dati e servizi ordinari

2.1 Interoperabilità e portabilità

2.1.1) Interoperabilità.

IP.IN-01: Sono disponibili API per funzionalità applicative

1_O. *Il servizio SaaS espone opportune API di tipo SOAP e/o REST verso l'Amministrazione associate alle funzionalità applicative, prevedendo in particolare la tracciabilità delle versioni disponibili e la tracciabilità delle richieste ricevute ed evase. Inoltre, è disponibile documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint. [SaaS].*

2.1.2) Gestione remota.

IP.GR-01: Sono disponibili API per la gestione remota del ciclo di vita del servizio

1_O. *Coerentemente con la tipologia di servizio cloud erogato, l'ambiente dello stesso deve essere accessibile tramite delle interfacce API per la gestione remota dei servizi, assicurando che le API esposte consentano l'implementazione di strumenti per la gestione automatica e remota del ciclo di vita del servizio cloud.*

2_O. *È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.*

3_O. *Con riferimento ai punti 1_O. e 2_O., deve essere prevista la retrocompatibilità delle diverse versioni delle API con quella disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.*

2.1.3) Portabilità.

IP.PO-01: Sono disponibili funzionalità/API per import/export dei dati

1_O. *Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.*

IP.PO-02: L'interoperabilità e la portabilità dei dati sono gestite mediante procedure e politiche regolarmente aggiornate. La portabilità dei dati prevede l'applicazione di protocolli di rete sicuri e l'accesso ai dati al termine dei rapporti contrattuali è gestito mediante accordi specifici.

1_O. *Sono definite politiche e procedure per l'interoperabilità e la portabilità, le quali vengono riviste e aggiornate almeno su base annuale, compresi requisiti per:*

a. Comunicazioni tra le interfacce delle applicazioni;

b. Interoperabilità del trattamento delle informazioni;

c. Portabilità dello sviluppo di applicazioni;
d. Scambio, uso, portabilità, integrità e persistenza delle informazioni/dati. [PaaS, SaaS].

2_O. *Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS].*

3_O. *Sono incluse, all'interno degli accordi disposizioni che specifichino l'accesso dell'Amministrazione ai dati al termine del contratto, inclusi:*
a. Formato dei dati;
b. Durata del tempo in cui i dati saranno conservati;
c. Portata dei dati conservati e messi a disposizione dell'Amministrazione;
d. Politica di cancellazione dei dati. [PaaS, SaaS].

2.2 Performance e scalabilità

2.2.1) Caratteristiche del servizio.

PS.CA-01: Il servizio cloud presenta le caratteristiche tipiche ed è conforme agli standard di settore

1_O. *Il servizio cloud garantisce almeno le seguenti caratteristiche, come da indicazioni NIST SP 800-145:*
a. self-service provisioning: il servizio cloud provvede unilateralmente alla fornitura delle risorse informatiche (ad esempio, server e storage in cloud), secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Il servizio cloud soddisfa unilateralmente le richieste dell'Amministrazione di risorse computazionali (o informatiche), senza esplicita verifica o approvazione;
b. accesso alla rete: il servizio cloud offre opzioni multiple di connettività alla rete; di cui almeno una basata su rete pubblica (es., Internet);
c. elasticità: il soggetto implementa meccanismi automatici di provisioning e de-provisioning del servizio, salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.

2.2.2) Scalabilità del servizio.

PS.SC-01: Trasparenza sulle modalità e meccanismi di scalabilità

1_O. *Il soggetto comunica all'Amministrazione:*
a. il meccanismo di scalabilità offerto (es. automatico e configurabile, nativo, manuale);
b. la tipologia (orizzontale e/o verticale);
c. le condizioni massime di carico sopportabili dal servizio (es. numero di utenti concorrenti e/o volume di richieste processabili);
d. le modalità di configurazione (es. sulla base di metriche di monitoraggio, pianificato nel tempo);
e. i tempi minimi di reazione del servizio alla richiesta di nuove risorse (es, attivazione di nuove risorse).

2_O. *Il fornitore rende disponibili all'Amministrazione informazioni trasparenti in merito ad eventuali ulteriori funzionalità accessorie disponibili per il servizio e configurabili dall'Amministrazione acquirente per gestire la scalabilità ed ottenere parametri migliori.*

3_O. *Per tutte le API esposte dal servizio cloud deve essere dichiarata la conformità al Modello di interoperabilità, definito da AgID con le linee guida adottate ai sensi della normativa vigente.*
Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).

2.3 Qualità

2.3.1) Livello del servizio (SLA).

QU.LS-01: È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative

1_O. *Il soggetto garantisce l'aderenza agli obiettivi (Minimum Service Level Objective - SLO) corrispondenti ai seguenti indicatori di servizio (Service Level Indicator - SLI) e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA):*
a. disponibilità pari al 99%, dove la disponibilità è intesa come la percentuale di tempo in un mese in cui il servizio cloud risulta essere accessibile e usabile, specificando che il tempo totale del periodo

di riferimento, che funge da base di calcolo del dato percentuale, non tiene conto degli eventi catastrofici (per eventi catastrofici si intendono eventi che rendono indisponibili per un periodo di tempo prolungato le infrastrutture impiegate per l'erogazione del servizio e al verificarsi dei quali è attivata la soluzione di Disaster Recovery);

b. "supporto tecnico per emergenze", relativo all'orario in cui il servizio di supporto tecnico è operativo per emergenze: 24 ore al giorno, 7 giorni a settimana per tutto l'anno;

c. un tempo massimo di risposta agli incidenti (inteso come tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta da parte del soggetto) pari a 1 ora;

d. "minor release", inteso come l'intervallo di tempo minimo di preavviso previsto per dare comunicazione, accompagnata da release note, alla Amministrazione di Minor Release (per Minor Release si intendono modifiche al servizio che riguardano principalmente correzioni di malfunzionamenti del software - bug - o comunque aggiunta di nuove funzionalità retro compatibili): 3 giorni;

e. "major release", inteso come l'intervallo di tempo minimo di preavviso previsto per dare comunicazione, accompagnata da release note, alla Amministrazione di Major Release (per Major Release si intendono modifiche al servizio che riguardano una sostanziale evoluzione delle funzionalità del servizio rispetto alla versione precedente): 1 mese.

2_O. *Rispetto a quelli riportati al punto 1_O., il soggetto può comunicarne all'amministrazione eventuali ulteriori, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici Minimum Service Level Objective (SLO) nei rapporti contrattuali.*

3_O. *Il soggetto garantisce che venga definita la modalità di condivisione delle informazioni dei livelli di servizio atteso garantiti (SLA) del servizio cloud con l'amministrazione (es. report periodico) e che, qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'amministrazione per ottenerne la sua approvazione.*

QU.LS-02: Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione

1_O. *All'interno dei Service Level Agreement (SLA) tra il soggetto e l'amministrazione sono presenti limitazioni con riferimento a modifiche che abbiano impatto direttamente sugli ambienti e/o tenant di proprietà dell'amministrazione.*

QU.LS-03: Esistono contenuti e caratteristiche minimi per i Service Level Agreement

1_O. *Ogni SLA tra il soggetto e l'amministrazione tiene conto di quanto segue:*

a. Ambito, caratteristiche e ubicazione della relazione commerciale e dei servizi offerti;

b. Requisiti di sicurezza delle informazioni (incluso il SSRM - Shared Security Responsibility Model, se applicabile);

c. Processo di Change Management;

d. Logging e Monitoring;

e. Gestione degli incidenti e procedure di comunicazione;

f. Diritto di audit e valutazione da parte di terzi;

g. Modalità di cessazione del servizio;

h. Requisiti di interoperabilità e portabilità;

i. Riservatezza dei dati.

QU.LS-04: È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato

1_O. *Il soggetto rende disponibile all'amministrazione l'accesso ad uno o più strumenti di monitoraggio per il servizio cloud. Essi devono consentire attività di raccolta, monitoraggio, filtraggio, creazione di report attraverso parametri predefiniti o parametrizzabili e consentire all'amministrazione di impostare allarmi personalizzati. La granularità massima delle operazioni non deve essere superiore al minuto (ad es., deve essere possibile filtrare o raccogliere gli eventi ogni minuto). In aggiunta, il soggetto*

specifica l'eventuale disponibilità di API e strumenti di monitoraggio di terze parti integrate nativamente con il servizio qualificato.

2.3.2) Qualità del servizio (SE).

QU.SE-01: Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore

- ***1_O.*** *Il sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN ISO 9001:2015-Sistemi di Gestione per la Qualità.*
- ***2_O.*** *Il sistema di gestione dei servizi IT del servizio cloud è adottato formalmente dal soggetto in conformità allo standard ISO/IEC 20000-1:2018-Sistema di gestione dei servizi IT.*

QU.SE-02: Viene fornito un adeguato servizio di assistenza e supporto

- ***1_O.*** *È garantito il servizio di supporto e assistenza tecnica all'amministrazione per il servizio cloud.*
- ***2_O.*** *Il servizio di supporto e assistenza di cui al punto 1_O. è fornito almeno in lingua inglese dalle 08.00 alle 18.00 (ora italiana) nei giorni lavorativi. Su richiesta dell'Amministrazione, il servizio di supporto e assistenza di cui al punto 1_O. è fornito almeno in lingua italiana e/o per un orario più esteso fino a coprire tutti giorni dell'anno a qualsiasi orario (24 ore al giorno, 7 giorni alla settimana per tutto l'anno).*
- ***3_O.*** *Il servizio di supporto e assistenza di cui al punto 1_O. è accessibile almeno tramite recapito telefonico e posta elettronica.*
- ***4_O.*** *Il servizio di supporto e assistenza di cui al punto 1_O. prevede, inoltre, un sistema di supporto alla risoluzione dei problemi (detto anche "troubleshooting") a disposizione dell'Amministrazione, rendendolo disponibile, su richiesta dell'amministrazione, tramite API al fine di permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).*

QU.SE-03: Il soggetto dichiara la frequenza di aggiornamento del servizio

- ***1_O.*** *Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).*

QU.SE-04: Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud

- ***1_O.*** *Devono essere rese disponibili all'amministrazione le linee guida per una gestione sicura del servizio cloud oggetto di qualificazione, indirizzando, ove applicabile, i seguenti aspetti:*
  a. Istruzioni per una configurazione sicura;
  b. Informazione su vulnerabilità note e meccanismi di aggiornamento;
  c. Gestione degli errori e meccanismi di logging;
  d. Meccanismi di autenticazione;
  e. Ruoli e diritti, comprese le combinazioni che risultano in un rischio elevato;
  f. Servizi e funzioni per l'amministrazione del servizio da parte di utenti privilegiati;
  g. Le linee guida vengono fornite e mantenute nelle modalità e tempistiche di cui alla misura IP.GR-01.

2.4 Sicurezza

IDENTIFY (ID)

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

ID.AM-01: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione

- ***1_O.*** *Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.*
- ***2_O.*** *Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.*

ID.AM-02: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione

- ***1_O.*** *Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.*
- ***2_O.*** *L'installazione delle piattaforme e delle applicazioni software è consentita esclusivamente per quelle approvate.*
- ***3_O.*** *Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione.*

ID.AM-03: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati

- ***1_O.*** *Tutti i flussi di dati e di informazioni, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati, censiti e approvati da attori interni al soggetto.*

ID.AM-06: 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_O.*** *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_O.*** *È nominato, nell'ambito dell'articolazione di cui al punto 1_O., un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.*
- ***3_O.*** *Sono nominati, nell'ambito dell'articolazione di cui al punto 1_O., 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 Italia ai fini della gestione degli incidenti aventi impatto sul servizio cloud.*
- ***4_O.*** *L'incaricato di cui al punto 2_O. e il referente tecnico di cui al punto 3_O. operano in stretto raccordo.*

2.4.2) 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.

ID.GV-01: È identificata e resa nota una policy di cybersecurity

- ***1_O.*** *Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.*
- ***2_O.*** *Il Documento di cui al punto 1_O. deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.*

ID.GV-04: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity

- ***1_O.*** *l documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity.*
- ***2_O.*** *Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy del cloud.*

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

ID.RA-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

- ***1_O.*** *Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica del servizio cloud e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione.*
- ***2_O.*** *Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).*

ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio

- ***1_O.*** *L'analisi del rischio è svolta 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_O.*** *L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud.*
- ***3_O.*** *Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.*

2.4.4) Supply Chain Risk Management (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.

ID.SC-01: 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_O.*** *Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber.*
- ***2_O.*** *Tali processi sono validati e approvati da parte dei vertici del soggetto.*

PROTECT (PR)

2.4.5) Identity Management, Authentication and Access Control (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.

PR.AC-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

- ***1_O.*** *Le credenziali di accesso sono individuali per il personale del soggetto o comunque coinvolto nell'amministrazione del servizio e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.*
- ***2_O.*** *Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1_O., le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.*
- ***3_O.*** *Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.*
- ***4_O.*** *Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).*
- ***5_O.*** *Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.*
- ***6_O.*** *Esiste una pianificazione aggiornata degli audit di sicurezza per verificare il rispetto di quanto previsto nei punti 1_O., 2_O., 3_O., 4_O. e 5_O. ed esiste un registro degli audit effettuati con la relativa documentazione.*

PR.AC-03: L'accesso remoto alle risorse è amministrato

- ***1_O.*** *Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.*
- ***2_O.*** *Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.*
- ***3_O.*** *È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.*
- ***4_O.*** *Esiste un log degli accessi eseguiti da remoto.*
- ***5_O.*** *Per gli accessi da remoto, sono impiegati modalità di autenticazione a fattore multiplo.*

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

- ***1_O.*** *Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, 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 a gruppi di utenti.

2_O. *Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.*

3_O. *Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.*

PR.AC-05: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

1_O. *Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.*

2_O. *È presente una pianificazione per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste.*

PR.AC-07: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, 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_O. *Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.*

2_O. *In relazione al servizio cloud, deve essere garantita all'Amministrazione la funzionalità di autenticazione a più fattori o l'uso di soluzioni di autenticazione a più fattori di terze parti. Devono essere rese disponibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori disponibili, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).*

2.4.6) Awareness and Training (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.

PR.AT-01: Il personale del soggetto è informato e addestrato

1_O. *Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti.*

2_O. *L'addestramento e la formazione di cui al punto 1_O. fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche:*

a. la tutela della confidenzialità di dati in chiaro o cifrati;

b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro;

c. la definizione di ruoli e delle responsabilità;

d. politiche di accesso a sistemi, asset e risorse;

e. politiche di gestione delle informazioni e della sicurezza;

f. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;

g. requisiti per la non divulgazione/confidenzialità di informazioni.

PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

1_O. *Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.*

2_O. *Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.*

2.4.7) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

1_O. *I dati dell'amministrazione, ivi inclusi quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Salvo motivate e documentate ragioni di natura normativa o tecnica, nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di:*

a. Business Continuity e Disaster Recovery, anche se esternalizzate (ad esempio tramite cloud computing);

b. Content Delivery Network con distribuzione geografica globale.

In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali.

2_O. *Diversamente dal caso dei Metadata relativi al funzionamento del Servizio, che possono essere trattati mediante infrastrutture localizzate anche al di fuori del territorio dell'Unione europea, i Metadata relativi all'amministrazione sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di Metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.*

3_O. *Con riferimento al punto 2_O., nel caso in cui i Metadata relativi all'amministrazione siano finalizzati all'erogazione di servizi per la sicurezza informatica ovvero per la resilienza dell'infrastruttura digitale, essi possono essere trattati, in presenza di motivate ragioni tecniche e relative evidenze di una loro gestione conforme all'univocità delle finalità del trattamento, anche fuori del territorio europeo. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.*

4_O. *Sono definite, 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.

5_O. *Con riferimento alle chiavi crittografiche:*

a. esiste un documento aggiornato di dettaglio inerente alle procedure di crittografia, alla cifratura e alla gestione delle chiavi, le quali dovranno essere aggiornate almeno su base annuale, e recante un'indicazione puntuale di ruoli e responsabilità;

b. è prevista una verifica periodica di sistemi, politiche e processi di crittografia e gestione delle chiavi in risposta all'aumento dell'esposizione al rischio, valutato mediante audit da eseguire con cadenza almeno annuale o dopo qualsiasi evento di sicurezza;

c. è prevista la generazione di chiavi crittografiche mediante l'utilizzo di librerie crittografiche, con un'indicazione in merito all'algoritmo e al generatore di numeri casuali utilizzati;

d. sono previsti meccanismi di rotazione delle chiavi crittografiche secondo il periodo di validità delle stesse, tenendo conto di possibili rischi e requisiti normativi e legali.

6_O. *Con riferimento alle chiavi crittografiche, su richiesta dell'amministrazione, il soggetto garantisce:*

a. la gestione autonoma da parte dell'amministrazione;

b. la generazione di chiavi crittografiche segrete e private per uno scopo unico.

7_O. *Sono presenti processi, procedure e misure tecniche per revocare e rimuovere le chiavi crittografiche prima della fine del loro periodo di validità, quando una chiave è compromessa, o un'entità non fa più parte dell'organizzazione, conformemente a requisiti legali e normativi, coerentemente con quanto previsto nei punti 5_O. e 6_O..*

8_O. *Sono definiti e implementati processi, procedure e misure per la creazione, disattivazione di chiavi al momento della scadenza, eventuali sospensioni e meccanismi di gestione per le chiavi crittografiche, coerentemente con quanto previsto nei punti 5_O. e 6_O..*

PR.DS-02: I dati sono protetti durante la trasmissione

1_O. *Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.*

PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

1_O. *Sono definite in relazione alla categoria ID.AM:*

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.

PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)

1_O. *Sono definite 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.

2_O. *Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.*

PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

1_O. *Sono definiti 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.

PR.DS-07: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

1_O. *Sono definite in relazione alla categoria ID.AM:*

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.

2.4.8) Information Protection Processes and Procedures (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.

PR.IP-01: 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_O. *Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale. [IaaS, SaaS].*

PR.IP-03: Sono attivi processi di controllo della modifica delle configurazioni

1_O. *Sono definite:*

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.

2_O. *È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.*

3_O. *Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.*

PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati

1_O. *Sono definite, 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.

2_Oa. *Viene effettuato periodicamente un backup dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup.*

2_Ob. *Viene effettuato periodicamente un backup delle informazioni memorizzate nel cloud necessarie per il completo ripristino del sistema, ivi incluso i dati dell'Amministrazione e i dati necessari per il ripristino del servizio. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup. A tal fine, viene anche assicurato che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.*

3_O. *Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette adottando standard crittografici allo stato dell'arte e migliori pratiche di settore, ed archiviate regolarmente in siti remoti (nel rispetto di quanto previsto dalla categoria PR.DS). Qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta adottando standard crittografici allo stato dell'arte e migliori pratiche di settore.*

4_O. *Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come obiettivo (SLO) almeno 1 volta all'anno.*

PR.IP-09: 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_O. *L'impatto derivante da interruzioni di business ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.*

2_O. *Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta 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 Italia.

3_O. *Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.*

4_O. *I piani di business continuity sono collaudati e comunicati alle parti interessate.*

5_O. *La documentazione di cui al punto 2_O. è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.*

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

1_O. *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.

2_O. *Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale. [SaaS].*

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

PR.MA-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

1_O. *Sono definite 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.*

PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

1_O. *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-03 e dei seguenti punti.*

2_O. *Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.*

3_O. *Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.*

4_O. *Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.*

5_O. *Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.*

2.4.10) Protective Technology (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.

PR.PT-01: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

1_O. *I log son conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.*

2_O. *Sono definite:*
- *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.*

PR.PT-04: Le reti di comunicazione e controllo sono protette

1_O. *I sistemi perimetrali, quali firewall, anche a livello applicativo (ivi inclusi Web Application Firewall), sono presenti, aggiornati, manutenuti e ben configurati.*

PR.PT-05: 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_O. *In relazione ai piani previsti dalla sottocategoria PR.IP-09:*
- *a. sono adottate architettura ridondate di rete, di connettività, nonché applicative.*

2_O. *Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza previste.*

3_O. *Sono definite:*
- *a. le politiche di sicurezza adottate in relazione ai punti 1_O. e 2_O;*
- *b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.*

DETECT (DE)

2.4.11) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

- ***1_O.*** *Ai fini di rilevare tempestivamente incidenti con impatto sul servizio cloud, sono adottati gli strumenti tecnici e procedurali per:*
  - *a. acquisire le informazioni da più sensori e sorgenti;*
  - *b. ricevere e raccogliere informazioni inerenti alla sicurezza del servizio cloud rese note dal CSIRT Italia, da fonti interne o esterne al soggetto;*
  - *c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a. e b., per rilevare tempestivamente eventi di interesse.*
- ***2_O.*** *Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La documentazione relativa alle attività di analisi e investigazione dell'evento, anche elettronica, e conservata per almeno 24 mesi.*
- ***3_O.*** *Sono definite:*
  - *a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1_O., lettera a.;*
  - *b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1_O., lettere a. e b.;*
  - *c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1_O., lettera c-;*
  - *d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2_O.*
- ***4_O.*** *Sono presenti politiche e procedure di logging, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.*
- ***5_O.*** *È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati.*
- ***6_O.*** *Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile.*
- ***7_O.*** *Nell'ambito delle attività di logging e monitoraggio, in relazione al servizio cloud sono forniti strumenti di gestione degli errori e logging che consentono all'Amministrazione di definire il periodo di custodia (retention) desiderato e di ottenere informazioni sullo stato di sicurezza del servizio cloud, nonché sui dati e le funzioni che fornisce. Le informazioni devono essere sufficientemente dettagliate da consentire la verifica dei seguenti aspetti, nella misura in cui sono applicabili al servizio cloud:*
  - *a. Quali dati, servizi o funzioni disponibili per l'utente all'interno del servizio cloud sono stati consultati da chi e quando (Audit Logs);*
  - *b. Malfunzionamenti durante l'elaborazione di azioni automatiche o manuali.*
- ***8_O.*** *Per il servizio oggetto di qualificazione deve essere garantita la possibilità di integrare i log nel sistema SIEM di gestione e monitoraggio dell'Amministrazione e che i file di log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.*

2.4.12) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

DE.CM-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

- ***1_O.*** *Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS).*
- ***2_O.*** *Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.*
- ***3_O.*** *È previsto un sistema di monitoraggio degli accessi al fine di rilevare attività sospette e stabilire un processo definito per l'adozione di azioni appropriate e tempestive in risposta alle anomalie rilevate.*

DE.CM-04: Il codice malevolo viene rilevato

- ***1_O.*** *Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection System - EPS).*
- ***2_O.*** *Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.*

DE.CM-08: Vengono svolte scansioni per l'identificazione di vulnerabilità

1_O. *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.*

2.4.13) Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.

DE.DP-01: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability

1_O. *Le nomine di cui alla sottocategoria ID.AM-06 sono rese note all'interno del soggetto.*

2_O. *I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto.*

3_O. *Esiste un documento aggiornato di dettaglio che indica almeno:*
a. i ruoli, i processi e le responsabilità di cui al punto 2_O.;
b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1_O. e 2_O.

4_O. *È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate [PaaS, SaaS].*

RESPOND (RS)

2.4.14) Response Planning (RS.RP) Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

RS.RP-01: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente

1_O. *Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DETECT (DE) nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sul servizio cloud.*

2.4.15) Communications (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).

RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

1_O. *I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di risposta ad un incidente sono ben definiti e resi noti alle articolazioni competenti del soggetto.*

2_O. *Sono eseguite periodicamente esercitazioni.*

3_O. *Esiste un documento aggiornato di dettaglio che indica almeno:*
a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1_O. e 2_O.;
b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1_O. e 2_O.;
c. le modalità per le esercitazioni di cui al punto 2_O..

4_O. *Il soggetto provvede a notificare l'Amministrazione di un incidente o data breach entro 1 ora dalla registrazione e classificazione dell'evento.*

RS.CO-05: è attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awarenesss)

1_O. *Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e alla cyber sicurezza, nonché con altre entità rilevanti in linea con il contesto del soggetto.*

2_O. *Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.*

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

RS.AN-05: 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_O.*** *Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei penetration test e vulnerability assessment di cui alla sottocategoria DE.CM-08 sono diffusi alle articolazioni competenti del soggetto.*
- ***2_O.*** *I canali di comunicazione del CSIRT Italia 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 (ISAC) di riferimento sono monitorati.*
- ***3_O.*** *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_O. e 2_O.;*
  - *b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1_O. e 2_O..*

2.4.17) Mitigation (RS.MI)Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente.

RS.MI-03: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

- ***1_O.*** *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.*

RECOVER (RC)

2.4.18) Recovery Planning (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.

RC.RP-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity

- ***1_O.*** *Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento dei servizi cloud coinvolti da un incidente di cybersecurity.*

3. Caratteristiche di base previste nel caso di dati e servizi critici

3.1 Qualità

3.1.1) Qualità del servizio (SE)

QU.SE-02: Viene fornito un adeguato servizio di assistenza e supporto

- ***5_C.*** *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni della misura QU.SE-02, punto 2_O. Il servizio di supporto e assistenza di cui al punto 1_O. è fornito almeno in lingua italiana tutti i giorni dell'anno a qualsiasi orario (24 ore al giorno, 7 giorni alla settimana per tutto l'anno).*

3.2 Sicurezza

IDENTIFY (ID)

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

ID.AM-06: 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)

- ***5_C.*** *I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2_O. e del referente tecnico di cui al punto 3_O. sono comunicati dal soggetto all'Agenzia per la cybersicurezza nazionale (ACN).*

6_C. *Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.*

7_C. *Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2_O. e al referente tecnico di cui al punto 3_O. presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.*

8_C. *L'incaricato di cui al punto 2_O. assicura, inoltre, la collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82 del 2021.*

3.2.2) 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.

ID.GV-01: È identificata e resa nota una policy di cybersecurity

3_C. *Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1_O. deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato.*

4_C. *Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti.*

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

ID.RA-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

3_C. *Le relazioni periodiche delle verifiche e dei test di cui al punto 1_O. 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.

4_C. *Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.*

ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio

4_C. *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 alla sottocategoria DE.CM-8;

c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati;

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

3.2.4) Supply Chain Risk Management (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.

ID.SC-01: 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

3_C. *All'interno dell'organizzazione, sono presenti ed aggiornate almeno su base annuale le politiche e le procedure per la definizione, implementazione e applicazione del modello di responsabilità della*

sicurezza condivisa rispetto a soggetti esterni e/o Amministrazioni terze (Shared Security Responsibility Model-SSRM).

4_C. *Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione.*

5_C. *È fornita una chiara definizione in merito alla condivisione delle responsabilità.*

ID.SC-02: 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_C. *In merito all'affidamento di forniture per i servizi cloud sono adottate misure in materia di sicurezza della catena di approvvigionamento cyber attraverso:*

a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-06, punto 2_O., 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 servizio cloud;

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_C. *Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1_C..*

ID.SC-03: 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_C. *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 servizio cloud. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.*

ID.SC-04: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1_C. *Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.*

2_C. *Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.*

3_C. *È definito ed implementato un processo di Audit Management al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio.*

4_C. *Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.*

5_C. *È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation, relativo alle le azioni correttive connesse alle non conformità rilevate sui fornitori e partner terzi.*

PROTECT (PR)

3.2.5) Identity Management, Authentication and Access Control (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.

PR.AC-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

7_C. *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 le procedure di cui ai punti 1_O., 2_O., 3_O., 4_O., 5_O., 6_O.;

b. 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;

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

PR.AC-03: L'accesso remoto alle risorse è amministrato

6_C. *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. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

4_C. *Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1_O..*

3.2.6) Awareness and Training (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.

PR.AT-01: Il personale del soggetto è informato e addestrato

3_C. *Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.*

3.2.7) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

9_C. *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui al punto 6_O. Con riferimento alle chiavi crittografiche, il soggetto garantisce la gestione autonoma da parte dell'Amministrazione e la generazione di chiavi crittografiche segrete e private per uno scopo unico e garantisce la conformità ai requisiti di cui ai punti 7_O. e 8_O. coerentemente.*

10_C. *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.

11_C. *Il servizio cloud supporta un meccanismo di cifratura di tipo Bring Your Own Key (BYOK), che consente all'Amministrazione di generare autonomamente almeno la chiave principale di cifratura (root key), attraverso un HSM ospitato, alternativamente, presso:*

a. propria infrastruttura;

b. infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata;

c. infrastruttura di una terza parte scelta dall'Amministrazione.

12_C. *Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui punto 3_0. Con riferimento al trattamento dei metadati relativi all'amministrazione, resta fermo, pertanto, quanto previsto dal punto 2_O..*

13_C. *Sono definite ed implementate procedure e misure tecniche per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono più necessari, in conformità con requisiti legali e normativi.*

14_C. *Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 12_C. nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud.*

PR.DS-02: I dati sono protetti durante la trasmissione

2_C. *Conformemente all'analisi del rischio di cui alla misura ID.RA-05, per i flussi di dati e le comunicazioni di cui alla misura ID.AM-03 sono utilizzati canali di comunicazione sicuri e criptati e protocolli aggiornati e approvati.*

PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

2_C. *Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti che, qualora compromessi, possano avere impatti sulla disponibilità del servizio o sulla disponibilità, integrità o confidenzialità dei dati ad esso connessi.*

3_C. *Coerentemente con quanto previsto dal punto 2_C., sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto.*

3.2.8) Information Protection Processes and Procedures (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.

PR.IP-01: 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)

2_C. *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 il dispiegamento delle sole configurazioni adottate;

b. l'elenco delle configurazioni dei sistemi IT e 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. [SaaS].

3_C. *Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.*

4_C. *Sono definite ed implementate metriche, di natura tecnica, utili a monitorare il livello di aderenza ai requisiti di sicurezza definiti e gli obblighi di conformità.*

5_C. *Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile.*

6_C. *È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS].*

7_C. *È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].*

PR.IP-02: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle)

1_C. *Sono implementate linee guida e misure tecniche/organizzative per lo sviluppo sicuro del servizio cloud, in aderenza alle linee guida OWASP in merito alla sicurezza nello sviluppo del software (requisiti, progettazione, implementazione, test e verifica). Devono essere resi disponibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e alla Amministrazione i report sui test OWASP condotti, garantendo l'assenza di vulnerabilità di tipo "high" o "critical".*

PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati

5_C. 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.

6_C. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1_O..

PR.IP-09: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro

6_C. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal servizio cloud e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di disaster recovery.

7_C. Esiste un documento aggiornato di dettaglio contenente i piani di 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 Italia.

8_C. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.

9_C. Le strategie di disaster recovery sono collaudate e comunicate alle parti interessate.

10_C. I dispositivi critici per il funzionamento del servizio cloud sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore.

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

3_C. Sono definite ed implementate misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti o open, nel rispetto delle politiche interne di vulnerability management.

4_C. Il documento di cui al punto 1_O. della misura PR.IP-12 dovrà essere aggiornato su base semestrale.

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

PR.MA-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

2_C. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O.

3_C. Le attività di cui al punto 1_O. sono volte a verificare anche aspetti di sicurezza.

4_C. Gli aggiornamenti software sono consentiti solo da fonti pre-autorizzate.

5_C. Tutti i log relativi alle attività di manutenzione e aggiornamento sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze che svolgono tali attività.

6_C. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 3_C., 4_C. e 5_C..

3.2.10) Protective Technology (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.

PR.PT-04: Le reti di comunicazione e controllo sono protette

2_C. Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.

3_C. Gli strumenti tecnici di cui ai punti 1_O. e 2_C. concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.

PR.PT-05: 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

4_C. *In relazione ai piani previsti dalla sottocategoria PR.IP-09:*
a. esiste un sito di disaster recovery, con caratteristiche coerenti con l'analisi del rischio.

DETECT (DE)

3.2.11) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato

DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

9_C. *Esiste un repository centralizzato che contiene i log di accesso degli utenti del soggetto, gestito direttamente dal soggetto e segregato a livello logico rispetto ai sistemi a cui terze parti hanno accesso diretto.*

3.2.12) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione

DE.CM-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

4_C. *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.*

5_C. *Gli strumenti tecnici di cui ai punti 1_O., 2_O., 3_O. e 4_C. sono aggiornati, manutenuti 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.*

6_C. *Gli strumenti tecnici di cui ai punti 1_O., 2_O., 3_O. e 4_C. sono impiegati anche per i fini di cui alla categoria DE.AE.*

7_C. *Esiste un documento aggiornato che descrive, almeno:*
a. le politiche di sicurezza adottate in relazione ai punti 1_O., 2_O., 3_O. e 4_C. ;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DE.CM-04: Il codice malevolo viene rilevato

3_C. *Sono configurati appositi software firewall su tutti i dispositivi.*

4_C. *I file in ingresso (tramite posta elettronica, download, dispositivi removibili, etc.) sono analizzati, anche tramite sandbox.*

5_C. *Gli strumenti tecnici di cui ai punti 1_O., 3_O. e 4_C. 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_C. *Esiste un documento aggiornato che descrive, almeno:*
a. le politiche di sicurezza adottate in relazione ai punti 1_O., 3_C. e 4_C. ;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DE.CM-07: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

1_C. *Con riferimento alla sottocategoria PR.AC-03, 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_C. *Con riferimento alla sottocategoria ID.AM-01, 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_C. *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. 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_C. *Esiste un documento aggiornato che descrive, almeno:*

a. le politiche di sicurezza adottate in relazione ai punti 1_O. e 2_C.;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DE.CM-08: Vengono svolte scansioni per l'identificazione di vulnerabilità

1_C. *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_C. *Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software, di cui al punto 1_O..*

3_C. *Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.*

4_C. *Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.*

RESPOND (RS)

3.2.13) Response Planning (RS.RP) Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.

RS.RP-01: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente

2_C. *Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.*

3_C. *Il piano di risposta e le politiche e procedure di cui ai punti 1_O. e 2_C. includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.*

4_C. *I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi.*

5_C. *Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity.*

6_C. *Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.*

7_C. *Deve essere implementato un Computer Emergency Response Team (CERT), a coordinamento della fase di risoluzione degli incidenti e in aderenza a quanto definito dalle linee guida ISO/IEC 27035-2. Inoltre, deve essere previsto il coinvolgimento periodico dell'Amministrazione in momenti di condivisione e revisione dello stato degli incidenti di interesse e, ove opportuno, nella risoluzione di tali incidenti, anche secondo gli accordi contrattuali in materia.*

3.2.14) Communications (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).

RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

5_C. *Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (lessons learned).*

6_C. *Sono presenti politiche e procedure per la gestione degli incidenti di sicurezza, E-Discovery e Cloud Forensics, le quali dovranno essere riviste e aggiornate almeno su base annuale.*

7_C. *Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.*

8_C. *È previsto un meccanismo di segnalazione per ogni violazione della sicurezza, reale o presunta, comprese eventuali violazioni inerenti la supply chain, nel rispetto di SLA, leggi e regolamenti applicabili.*

9_C. *Le attività di risposta condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione.*
In particolare, 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 interlocuzione con il CSIRT Italia.

3.2.15) Mitigation (RS.MI)Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente.

RS.MI-03: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

1_C. *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.*

2_C. *Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.*

RECOVER (RC)

3.2.16) Recovery Planning (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

RC.RP-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity

2_C. *Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.*

3.2.17) Communications (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).

RC.CO-03: 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_C. *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).*

4. Caratteristiche di base previste nel caso di dati e servizi strategici

4.1 Sicurezza

IDENTIFY (ID)

4.1.1) Supply Chain Risk Management (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

ID.SC-01: 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

6_S. *Esiste un documento recante i processi di cui ai punti 1_O. e 2_O..*

ID.SC-02: 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

3_S. *Si raccomanda, ove possibile e in relazione alla criticità di:*

a. valutare l'affidabilità tecnica di cui al punto 1_C., 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 ed eseguito;

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.

ID.SC-03: 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

2_S. *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 servizio cloud. A tal fine, contratti, accordi o convenzioni sono aggiornati di conseguenza.*

PROTECT (PR)

4.1.2) Identity Management, Authentication and Access Control (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.

PR.AC-03: L'accesso remoto alle risorse è amministrato

7_S. *Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione.*

8_S. *È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati dello stesso. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati.*

9_S. *Tutte le operazioni che prevedono l'accesso ai dati dell'Amministrazione devono essere gestite in linea con i criteri di user management e logging delle utenze privilegiate.*

PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

5_S. *Tutte le attività privilegiate (es. installazione di aggiornamenti) e di accesso ai dati dell'Amministrazione da parte del personale del soggetto e di terze parti dovranno essere autorizzati dall'organizzazione di cybersecurity e limitate ai soli casi essenziali.*

PR.AC-05: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

3_S. *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 use sono limitati e/o monitorati.

PR.AC-07: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, 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)

3_S. *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.

4.1.3) Awareness and Training (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.

PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

3_S. *Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1_O. e 2_O.*

4.1.4) Data Security (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.

PR.DS-01: I dati memorizzati sono protetti

15_S. *Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto:*

a. segnala all'Agenzia per la cybersicurezza nazionale (ACN) e all'amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE;

b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'amministrazione.

16_S. *Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio cloud. II soggetto rende disponibile l'elenco all'amministrazione.*

17_S. *Nel caso di dati e di servizi strategici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui punto 2_0. Al riguardo, tutte le tipologie di metadata devono essere trattate mediante infrastrutture localizzate sul territorio dell'Unione europea, ad eccezione di quelli necessari all'erogazione dei servizi indicati al punto 1_O..*

PR.DS-03: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

4_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)

3_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

2_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

PR.DS-07: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

2_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

4.1.5) Information Protection Processes and Procedures (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.

PR.IP-03: Sono attivi processi di controllo della modifica delle configurazioni

4_S. *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1_O..*

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

PR.MA-01: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

7_S. *Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.*

8_S. *In base all'analisi del rischio, ogni aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.*

9_S. *Il codice oggetto relativo agli aggiornamenti di cui al punto 4_C. viene custodito per almeno 24 mesi.*

PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

6_S. *Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2_O., 3_O., 4_O. e 5_O..*

4.1.7) Protective Technology (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.

PR.PT-01: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

- ***3_S.*** *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2_O.*

PR.PT-04: Le reti di comunicazione e controllo sono protette

- ***1_S.*** *I sistemi perimetrali, quali firewall, anche a livello applicativo (ivi inclusi Web Application Firewall), sono presenti, aggiornati, manutenuti e ben configurati.*
- ***2_S.*** *Sistemi di prevenzione delle intrusioni (intrusion prevention systems - IPS) sono presenti, aggiornati, manutenuti e ben configurati.*
- ***3_S.*** *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. concorrono al rispetto delle politiche di cui alla categoria ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.*
- ***4_S.*** *L'aggiornamento, manutenzione e configurazione degli strumenti tecnici di cui ai punti 1_O. e 2_C. sono effettuati nel rispetto delle politiche di cui alla categoria PR.AC, PR.DS, PR.IP e PR.MA.*
- ***5_S.*** *Gli strumenti tecnici di cui ai punti 1_O. e 2_C. sono impiegati anche per i fini di cui alla funzione DETECT (DE).*
- ***6_S.*** *Esiste un documento aggiornato che descrive almeno i processi e gli strumenti tecnici impiegati per realizzare i punti 1_O., 2_C., 3_C. e 4_S..*

PR.PT-05: 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

- ***5_S.*** *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2_O..*

DETECT (DE)

4.1.8) Anomalies and Events (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.

DE.AE-03: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

- ***10_S.*** *Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3_O..*

4.1.9) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.

DE.CM-07: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

- ***5_S.*** *Con riferimento alla sottocategoria ID.AM-02, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.*
- ***6_S.*** *Con riferimento alla sottocategoria ID.AM-03, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.*
- ***7_S.*** *Gli strumenti tecnici di cui ai punti 5_S. e 6_S. 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.*
- ***8_S.*** *Esiste un documento aggiornato che descrive, almeno:*
  a. le politiche di sicurezza adottate in relazione ai punti 5_S. e 6_S.;
  b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

RECOVER (RC)

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

RC.IM-02: Le strategie di recupero sono aggiornate

- ***1_S.*** *Il piano di cui alla sottocategoria RC.RP-01 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.*

5. **Caratteristiche di base con termini di applicazione differiti**

5.1. Si riporta di seguito l'elenco dei requisiti validi dopo sei mesi dalla data di applicazione del presente Regolamento:

- DE.CM-08.1_O.
- PR.AC-03.5_O.
- PR.IP-04.2_Ob.
- PR.PT-04.1_O.
- PR.PT-04.2_C.
- PR.PT-04.3_C.
- RS.MI-03.1_O.

REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LE PUBBLICHE AMMINISTRAZIONI, AI SENSI DELL'ARTICOLO 33-SEPTIES, COMMA 4, DEL DECRETO-LEGGE 18 OTTOBRE 2012, N. 179, CONVERTITO, CON MODIFICAZIONI, DALLA LEGGE 17 DICEMBRE 2012, N. 221

ALLEGATO 4

"REQUISITI PER L'ADEGUAMENTO E LA QUALIFICAZIONE DELLE INFRASTRUTTURE DIGITALI, INFRASTRUTTURE DEI SERVIZI CLOUD E DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE"

Sommario

1. **Premessa** 1
2. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 1 (AC1 e QC1)** 1
3. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 2 (AC2 e QC2)** 4
4. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 3 (AC3 e QC3)** 5
5. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 4 (AC4 e QC4)** 5
6. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 1 (AI1)** 6
7. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 2 (AI2)** 7
8. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 3 (AI3)** 7
9. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 4 (AI4)** 8

1. Premessa

1.1. Il presente Allegato definisce, in conformità alle previsioni di cui all'articolo 13 del Regolamento, i requisiti per l'adeguamento ai sensi dell'articolo 15 del Regolamento e per la qualificazione ai sensi dell'articolo 17 del Regolamento dei servizi cloud per le pubbliche amministrazioni che possono ospitare, rispettivamente, servizi e dati digitali della pubblica amministrazione classificati, ai sensi del processo di cui all'articolo 5 del Regolamento, quali ordinari, critici o strategici.

2. Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 1 (AC1 e QC1)

2.1. Caratteristiche dei servizi cloud

Ai fini della qualificazione di livello 1 (AC1 e QC1) è richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato 3 al presente Regolamento per i servizi cloud per le pubbliche amministrazioni che possono trattare dati e servizi classificati quali **ordinari** e dei requisiti addizionali definiti nelle successive sezioni, da 2.2 a 2.6.

2.2. Catena di adeguamento qualificazione dei servizi cloud

I servizi cloud per le pubbliche amministrazioni adeguati ai sensi dell'articolo 14 del

Regolamento ovvero qualificati ai sensi dell'articolo 17 del Regolamento sono erogati, quale livello sottostante, tramite un servizio cloud per le pubbliche amministrazioni qualificato o adeguato ovvero un'infrastruttura digitale o un'infrastruttura dei servizi cloud adeguata.

Al fine di adeguarsi ai sensi dell'articolo 14 del Regolamento ovvero ottenere una delle qualificazioni di cui all'articolo 17 del Regolamento per uno specifico livello, un servizio cloud per le pubbliche amministrazioni di tipo Infrastructure-as-a-Service (IaaS) deve essere erogato tramite:

a) un servizio cloud di tipo IaaS adeguato ovvero qualificato per il medesimo livello o superiore;
b) un'infrastruttura digitale per le pubbliche amministrazioni ovvero da una infrastruttura dei servizi cloud per le pubbliche amministrazioni adeguate ai sensi dell'articolo 12 del Regolamento, per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto a).

Al fine di adeguarsi ai sensi dell'articolo 14 del Regolamento ovvero ottenere una delle qualificazioni di cui all'articolo 17 del Regolamento per uno specifico livello, un servizio cloud di tipo Platform-as-a-Service (PaaS) deve essere erogato, alternativamente, tramite:

a) un servizio PaaS adeguato ovvero qualificato per il livello medesimo o superiore;
b) un servizio IaaS adeguato ovvero qualificato per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto a);
c) un'infrastruttura digitale per le pubbliche amministrazioni ovvero da una infrastruttura dei servizi cloud per le pubbliche amministrazioni adeguate ai sensi dell'articolo 12 del Regolamento, per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto b).

Al fine di adeguarsi ai sensi dell'articolo 14 del Regolamento ovvero ottenere una delle qualificazioni di cui all'articolo 17 del Regolamento per uno specifico livello, un servizio cloud di tipo Software-as-a-Service (SaaS) deve essere erogato, alternativamente, tramite:

a) un servizio SaaS adeguato ovvero qualificato per il livello medesimo o superiore;
b) un servizio SaaS sottostante, un servizio PaaS adeguato ovvero qualificato per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto a);
c) un servizio IaaS adeguato ovvero qualificato per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto b);
d) un'infrastruttura digitale per le pubbliche amministrazioni ovvero da una infrastruttura dei servizi cloud per le pubbliche amministrazioni adeguate ai sensi dell'articolo 12 del Regolamento, per il livello medesimo o superiore, ove il livello sottostante non sia rappresentato da un servizio di cui al punto c).

2.3. **Certificazioni richieste per fornitori privati nel caso di qualificazione di servizi cloud**

Ai fini della qualificazione di livello 1 (QC1) sono richieste:

- un'autocertificazione che attesti la conformità allo standard ISO 9001 – Sistemi di Gestione per la Qualità (SGQ). Il relativo campo di applicazione deve espressamente prevedere almeno le fasi di erogazione del servizio oggetto di qualifica e la prestazione del servizio di assistenza tecnica alla Pubblica Amministrazione italiana;
- la certificazione ISO/IEC 27001 – Sistema di gestione per la sicurezza delle Informazioni (SGSI) con estensioni ISO/IEC 27017 e ISO/IEC 27018 per il servizio cloud oggetto di qualifica, il cui perimetro di applicazione ("scope") deve riguardare almeno i processi relativi alla progettazione e all'erogazione dei servizi cloud oggetto di qualificazione. In alternativa al suddetto requisito è possibile presentare la certificazione *Cloud Security Alliance – Star Level 2*.

Per le istanze sottomesse dopo sei mesi dalla data di applicazione del presente Regolamento, le certificazioni devono essere emesse da ente certificatore accreditato da un organismo nazionale

di accreditamento di un paese membro dell'unione europea ovvero beneficiario di un accordo di mutuo riconoscimento con l'organismo nazionale di accreditamento italiano.

Le certificazioni dovranno eventualmente essere rinnovate al fine di coprire, senza soluzione di continuità, l'intero periodo di qualificazione.

2.4. **Ulteriori requisiti per servizi cloud erogati in prossimità**

Con riferimento ai servizi cloud che sono erogati in prossimità, il fornitore dei servizi cloud assicura l'implementazione dei seguenti requisiti aggiuntivi:

- oltre alla componente centrale, che dovrà rispettare tutti i requisiti previsti per la qualificazione ovvero l'adeguamento del servizio cloud, ai sensi degli articoli 17 e 14 del Regolamento, ivi inclusa la catena di qualificazione rispetto ad un'infrastruttura digitale ovvero un'infrastruttura dei servizi cloud adeguata, il servizio cloud può prevedere componenti locali su infrastrutture digitali, infrastrutture dei servizi cloud o infrastrutture di prossimità adeguate;
- in caso di una soluzione che permetta di scrivere localmente i dati degli applicativi (c.d. caching), tali dati sono trasferiti senza ingiustificato ritardo, anche attraverso operazioni programmate per gestire lotti massivi (ad es. scheduled job), presso uno o più repository Cloud. I dati primari, che l'applicazione deve utilizzare e di cui deve verificarne la correttezza, devono essere quelli presenti sulla componente centrale, mentre i dati presenti localmente devono essere esclusivamente di natura temporanea e ad uso e consumo per la gestione ordinaria. In particolare, in virtù della natura della soluzione, questa dovrà prevedere la memorizzazione dei dati trattati per il solo tempo necessario allo scopo ovvero configurabile a cura degli amministratori;
- ove non sussistano motivate giustificazione di natura tecnica ovvero normativa, tutte le operazioni CRUD (create, read, update, e delete) sulle informazioni devono essere fatte direttamente sul componente centrale che poi successivamente, se necessario, provvede a propagarlo sui sistemi locali;
- le modalità di funzionamento descritte nei punti precedenti dovranno essere verificate procedendo ad una cancellazione dei dati salvati in locale per poi andare a reperire le stesse informazioni dalla componente centrale, ricopiando in locale solo quanto strettamente necessario;
- la soluzione architetturale deve essere progettata e implementata senza comportare un detrimento dei requisiti di sicurezza previsti per la protezione del dato, anche a livello di rete locale. Inoltre, una volta completata la gestione, il dato deve poter essere cancellato, senza ingiustificato ritardo.

2.5. **Ulteriori requisiti nel caso di adeguamento di servizi cloud**

MON-01: Censimento utilizzo di servizi cloud *[Requisito applicabile dal 01/02/2025]*

1_O. *Il soggetto con servizi qualificati o adeguati comunica ad ACN, con cadenza semestrale, la lista delle amministrazioni che fanno uso dei propri servizi cloud, secondo le modalità rese disponibile sulla piattaforma digitale.*

2.6. **Ulteriori requisiti nel caso di qualificazione di servizi cloud**

MON-01: Censimento utilizzo di servizi cloud *[Requisito applicabile dal 01/02/2025]*

1_O. *Il soggetto con servizi qualificati o adeguati comunica ad ACN, con cadenza semestrale, la lista delle amministrazioni che fanno uso dei propri servizi cloud, secondo le modalità rese disponibile sulla piattaforma digitale.*

QU.LS-01: È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative

4_O. *Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura del servizio qualificato. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.*

5_O. *Per ogni contratto, il soggetto dispone garanzie assicurative adeguate per assicurare lo svolgimento di tutte le attività previste dall'articolo 21.*

QU.PR-01: Tracciamento, reportistica e trasparenza dei costi e della loro elaborazione

1_O. *Il soggetto rende disponibile all'amministrazione strumenti (es una dashboard) ed API che permettono di acquisire informazioni di dettaglio sulle metriche per il calcolo dei costi del servizio cloud (cd. di "billing") per rendere il calcolo trasparente all'amministrazione. Le metriche per il calcolo dei costi del servizio cloud devono essere espresse a livello sintetico o dettagliate per indirizzo di costo (es. risorsa cloud).*

2_O. *Gli strumenti e le API di cui al punto 1_O. permettono di filtrare e creare report di fatturazione con il dettaglio dei costi per ora, giorno o mese, per ogni account o prodotto in uso del servizio cloud. Il tracciamento e l'aggiornamento delle informazioni sul costo deve essere aggiornato almeno una volta ogni ora.*

QU.PR-02: Notifica e monitoraggio dei costi

1_O. *Il soggetto offre all'amministrazione un sistema di monitoraggio dei costi che permetta di impostare allarmi con notifiche per avvisare l'amministrazione nel caso in cui l'utilizzo del servizio cloud si avvicina o supera il budget/le soglie impostate.*

QU.PR-03: Requisiti minimi per il capitolato dei prezzi

1_O. *Il soggetto specifica all'amministrazione il proprio metodo e modello di determinazione dei prezzi per la fornitura del servizio cloud, che deve assicurare la massima flessibilità commerciale e supportare scalabilità e crescita.*

2_O. *Il soggetto fornisce all'amministrazione:*
a. un documento contenente i termini e le condizioni, specificando in particolare se i prezzi siano forniti per un servizio a consumo e se sono in atto politiche di adeguamento dinamico dei prezzi al mercato;
b. un documento contenente i prezzi (i riferimenti ai prezzi al pubblico sono ammessi a condizione che, su richiesta, sia disponibile un documento completo di listino/prezzi).

3. Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 2 (AC2 e QC2)

Ai fini della qualificazione di livello 2 (AC2 e QC2) è richiesto il rispetto dei requisiti per il livello di qualificazione di livello 1 (AC1 e QC1) e dei requisiti addizionali definiti nelle successive sezioni 3.1 e 3.2.

3.1. Caratteristiche dei servizi cloud

È richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato 3 del presente Regolamento per i servizi cloud per le pubbliche amministrazioni che possono trattare dati e servizi classificati quali **critici** ai sensi dell'articolo 3 del Regolamento.

3.2. Certificazioni richieste nel caso di qualificazione di servizi cloud

Ai fini della qualificazione di livello 2 (QC2) sono richieste:

- un'autocertificazione che attesti la conformità allo standard ISO 22301 – *Business Continuity Management System* (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica;
- un'autocertificazione che attesti la conformità allo standard ISO 20000 – *Service Management*

System per il servizio cloud oggetto di qualifica.

4. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 3 (AC3 e QC3)**

Ai fini della qualificazione di livello 3 (AC3 e QC3) è richiesto il rispetto dei requisiti per il livello di qualificazione 2 (AC2 e QC2) e dei requisiti addizionali definiti nelle successive sezioni 4.1 e 4.2.

4.1. **Caratteristiche dei servizi cloud**

È richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato 3 al presente Regolamento per i servizi cloud per le pubbliche amministrazioni che possono trattare dati e servizi classificati quali **strategici** ai sensi dell'articolo 3 del Regolamento.

4.2. **Certificazioni richieste nel caso di qualificazione di servizi cloud**

Ai fini della qualificazione di livello 3 (QC3) sono richieste:

- la certificazione ISO 22301 - *Business Continuity Management System* (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica;
- la certificazione ISO*/IEC* 20000 *(Service Management)* per il servizio cloud oggetto di qualifica;
- la certificazione *Cloud Security Alliance - Star Level 2.*

Per le istanze sottomesse dopo sei mesi dalla data di applicazione del presente Regolamento, le certificazioni devono essere emesse da ente certificatore accreditato da un organismo nazionale di accreditamento di un paese membro dell'unione europea ovvero beneficiario di un accordo di mutuo riconoscimento con l'organismo nazionale di accreditamento italiano.

Le certificazioni dovranno eventualmente essere rinnovate al fine di coprire, senza soluzione di continuità, l'intero periodo di qualificazione.

5. **Requisiti per l'adeguamento e la qualificazione dei servizi cloud di livello 4 (AC4 e QC4)**

Ai fini della qualificazione di livello 4 (AC4 e QC4) è richiesto il rispetto dei requisiti per il livello di qualificazione 3 (AC3 e QC3) e dei requisiti definiti nella successiva sezione 5.1.

5.1. **Ulteriori requisiti di sicurezza**

ID.AM-03: I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati

2_SS. *Tutti i flussi per l'erogazione del servizio cloud sono soggetti a procedure di approvazione, di monitoraggio e di controllo concordati con l'amministrazione.*

PR.DS-01: I dati memorizzati sono protetti

18_SS. *Il servizio cloud supporta un meccanismo di cifratura di tipo Hold Your Own Key (HYOK), che consente all'amministrazione la generazione e la gestione autonoma di tutte le chiavi di cifratura attraverso un HSM ospitato, alternativamente, presso:*
a. la propria infrastruttura;
b. un'infrastruttura messa a disposizione dal fornitore all'amministrazione in modalità dedicata presso una terza parte scelta dall'amministrazione.

19_SS. *E' garantito l'accesso esclusivo da parte dell'amministrazione alle chiavi di cui al punto 1 e ai dati in chiaro dell'amministrazione.*

20_SS. *Il fornitore dei servizi cloud mette a disposizione dell'amministrazione un servizio di HSM in modalità dedicata.*

21_SS. *Il fornitore dei servizi cloud è autonomo nella fornitura del servizio cloud, disponendo di proprie capacità per operare l'infrastruttura fisica e logica sottostante. Per casi eccezionali e sulla base di documentate limitazioni di carattere tecnico, il fornitore dei servizi cloud può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.*

PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)

1_SS. *Il fornitore dei servizi cloud rende disponibile all'amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato al servizio cloud o ai dati dell'amministrazione.*

2_SS. *Il fornitore dei servizi cloud rende disponibile all'amministrazione l'elenco dei dipendenti con accesso privilegiato al servizio cloud o ai dati dell'amministrazione. L'amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il fornitore dei servizi cloud provvede nel senso tempestivamente.*

6. Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 1 (AI1)

Ai fini dell'adeguamento di livello 1 (AI1) è richiesto il rispetto dei livelli minimi di cui all'Allegato 2 al presente Regolamento per le infrastrutture digitali ovvero le infrastrutture dei servizi cloud per le pubbliche amministrazioni che possono trattare dati e servizi classificati quali **ordinari** ai sensi dell'articolo 3 e dei requisiti addizionali definiti nelle successive sezioni 6.1, 6.2 e 6.3.

6.1. Certificazioni richieste nel caso di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni da parte di soggetti privati

Ai fini dell'adeguamento di una infrastruttura dei servizi cloud di livello QI1, non di tipo *housing*, sono richieste:

- la certificazione ISO 9001 - Sistemi di Gestione per la Qualità (SGQ) per l'infrastruttura digitale oggetto di qualifica. Il relativo campo di applicazione deve prevedere almeno la prestazione del servizio di assistenza tecnica ai clienti;
- la certificazione ISO/IEC 27001 – Sistema di gestione per la sicurezza delle Informazioni (SGSI), il cui perimetro di applicazione ("scope") deve riguardare almeno i processi relativi alla gestione e alla manutenzione dell'infrastruttura oggetto di qualifica.

Per le istanze sottomesse dopo sei mesi dalla data di applicazione del presente Regolamento, le certificazioni devono essere emesse da ente certificatore accreditato da un organismo nazionale di accreditamento di un paese membro dell'unione europea ovvero beneficiario di un accordo di mutuo riconoscimento con l'organismo nazionale di accreditamento italiano.

Le certificazioni dovranno eventualmente essere rinnovate al fine di coprire, senza soluzione di continuità, l'intero periodo di qualificazione.

6.2. Ulteriori requisiti nel caso di adeguamento di infrastruttura digitale da parte di soggetti pubblici, in-house o società a controllo pubblico che gestiscono le infrastrutture digitali della pubblica amministrazione per espressa previsione normativa

MON-01: Censimento utilizzo infrastrutture *[Requisito applicabile dal 01/02/2025]*

1_O. *Il soggetto con infrastrutture adeguate comunica ad ACN, con cadenza semestrale, la lista delle amministrazioni che fanno uso delle proprie infrastrutture digitali, secondo le modalità rese disponibile sulla piattaforma digitale.*

S.DC-04: Data center – titoli di possesso dei locali

1_O. *L'amministrazione deve dimostrare che gli immobili in cui sono situati i Data Center devono essere nella disponibilità esclusiva dell'Ente sulla base di uno dei seguenti titoli di possesso:*

a. proprietà;

b. locazione/comodato da altra PA o Demanio;

c. leasing immobiliare con possibilità di riscatto;

d. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".

6.3. **Ulteriori requisiti nel caso di adeguamento di infrastruttura dei servizi cloud per le pubbliche amministrazioni per soggetti privati**

MON-01: Censimento utilizzo infrastrutture *[Requisito applicabile dal 01/02/2025]*

1_O. *Il soggetto con infrastrutture adeguate comunica ad ACN, con cadenza semestrale, la lista delle amministrazioni che fanno uso delle proprie infrastrutture digitali, secondo le modalità rese disponibile sulla piattaforma digitale.*

QU.LS-01: È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative

1_O. *Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura dell'infrastruttura. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.*

2_O. *Per ogni contratto, il soggetto dispone garanzie assicurative adeguate per assicurare lo svolgimento di tutte le attività previste dall'articolo 21 del Regolamento.*

6.4. **Ulteriori requisiti nel caso di adeguamento di infrastrutture di prossimità**

Fermo restando la necessità di assicurare i requisiti di protezione del dato, ove sussistano, per le peculiarità dell'infrastruttura di prossimità ovvero per la natura del supporto fornito ai servizi cloud per le pubbliche amministrazioni, specifiche motivazioni tecniche che richiedano deroghe, anche parziali, ai livelli minimi di cui all'Allegato 2, l'operatore di infrastrutture digitali né dà evidenza di dettaglio nella relazione di conformità di cui agli articoli 13 e 14 del Regolamento, descrivendo, altresì, l'eventuale modalità alternativa con cui raggiunge analogo obiettivo e le eventuali analisi del rischio connesse. In ogni caso, l'operatore di infrastrutture digitali assicura almeno il rispetto dei livelli minimi previsti nell'Allegato 2 di seguito riportati:

- in tema di "Capacità Elaborativa", il par. 2.2;
- in tema di "Data Center Security", il par. 2.3 e 3.2;
- in tema di "Risparmio energetico", il par. 2.4;
- in tema di "Sicurezza", il par. 2.5, 3.3 e 4.2, coerentemente con il livello di adeguamento richiesto, come dall' articolo 12 del Regolamento, ad eccezione dei requisiti PR.IP-04, PR.IP-09 e PR.PT-05.

7. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 2 (AI2)**

Ai fini dell'adeguamento di livello 2 (AI2) è richiesto il rispetto dei requisiti per il livello di adeguamento 1 (AI1) e dei requisiti addizionali definiti nelle successive sezioni 7.1 e 7.2.

7.1. **Livelli minimi delle infrastrutture digitali**

Ai fini dell'adeguamento di livello 2 (AI2) è richiesto, inoltre, il rispetto dei livelli minimi di cui all'Allegato 2 al presente Regolamento per le infrastrutture digitali ovvero le infrastrutture dei servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali **critici** ai sensi dell'articolo 3 del Regolamento.

7.2. **Certificazioni richieste nel caso di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni da parte di soggetti privati**

Ai fini dell'adeguamento di una infrastruttura dei servizi cloud di livello 2 (AI2), non di tipo *housing,* è richiesta un'autocertificazione che attesti la conformità allo standard ISO 22301 - *Business Continuity Management System* (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica.

8. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 3 (AI3)**

Ai fini dell'adeguamento di livello 3 (AI3) è richiesto il rispetto dei requisiti per il livello di adeguamento 2 (AI2) e dei requisiti addizionali definiti nelle successive sezioni 8.1 e 8.2.

8.1. **Livelli minimi delle infrastrutture digitali**

Ai fini dell'adeguamento di livello 3 (AI3) è richiesto, inoltre, il rispetto dei livelli minimi di cui all'Allegato 2 al presente Regolamento per le infrastrutture digitali ovvero le infrastrutture dei servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali **strategici** ai sensi dell'articolo 3 del Regolamento.

8.2. **Certificazioni richieste nel caso di adeguamento delle infrastrutture dei servizi cloud per le pubbliche amministrazioni da parte di soggetti privati**

Ai fini dell'adeguamento di una infrastruttura dei servizi cloud di livello 3 (AI3), non di tipo *housing*, è richiesta la certificazione ISO 22301 - *Business Continuity Management System* (Gestione della continuità operativa) per l'infrastruttura oggetto di qualifica.

Per le istanze sottomesse dopo sei mesi dalla data di applicazione del presente Regolamento, le certificazioni devono essere emesse da ente certificatore accreditato da un organismo nazionale di accreditamento di un paese membro dell'unione europea ovvero beneficiario di un accordo di mutuo riconoscimento con l'organismo nazionale di accreditamento italiano.

Nel caso di adeguamento di infrastrutture di prossimità, è fatta possibilità di derogare al rispetto del presente requisito, descrivendo, nella relativa relazione di conformità, le motivate ragioni tecniche e organizzative per cui non è possibile adempiere alla presente previsione, unitamente alla descrizione, corredata da relativa analisi del rischio, relativamente alle modalità alternative per supportare le esigenze di *Business Continuity*.

Le certificazioni dovranno eventualmente essere rinnovate al fine di coprire, senza soluzione di continuità, l'intero periodo di qualificazione.

9. **Requisiti per l'adeguamento di una infrastruttura digitale ovvero di una infrastruttura dei servizi cloud di livello 4 (AI4)**

Ai fini dell'adeguamento di livello 4 (AI4) è richiesto il rispetto dei requisiti per il livello di adeguamento 3 (AI3) e dei requisiti definiti nella sezione 9.1.

9.1. **Ulteriori requisiti di sicurezza**

PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)

1_SS. *L'operatore di infrastrutture digitali rende disponibile all'amministrazione la metodologia utilizzata per la verifica del personale (vetting process methodology) con accesso privilegiato all'infrastruttura o ai dati dell'amministrazione.*

2_SS. *L'operatore di infrastrutture digitali rende disponibile all'amministrazione l'elenco dei dipendenti con accesso privilegiato all'infrastruttura o ai dati dell'amministrazione. L'amministrazione può richiedere unilateralmente la rimozione di uno o più dipendenti dal citato elenco e il fornitore dei servizi cloud provvede nel senso tempestivamente.*