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

(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 L'ITALIA DIGITALE

Visto il decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 e, in particolare, l'articolo 33-septies che prevede il consolidamento e 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 14 giugno 2021, n. 82, convertito, con modificazioni, 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, lettera m-ter), che ha attribuito all'Agenzia per la cybersicurezza nazionale la qualificazione dei servizi cloud per la pubblica amministrazione, nonché l'articolo 17, comma 6, secondo cui "[...] Nelle more dell'adozione dei decreti di cui al comma 5, il regolamento 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, è adottato dall'AgID, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri";

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il "Codice in materia di protezione dei dati personali";

Visto il decreto legislativo 7 marzo 2005 n. 82, recante il "Codice dell'Amministrazione Digitale";

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 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";

Vista la legge 27 dicembre 2019, n. 160, recante "Bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022", e in particolare l'articolo 1 commi 610-611, recanti gli obiettivi di risparmio di spesa per il triennio 2020-2022 per il settore informatico e per i data center;

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");

Visto il decreto del Presidente del Consiglio dei Ministri del 17 luglio 2020 con il quale è stato approvato il Piano Triennale per l'informatica 2020-2022;

Viste le circolari dell'Agenzia per l'Italia Digitale (AgID) n. 1 del 14 giugno 2019 recante il "censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali", n. 2 del 9 aprile 2018, recante i "Criteri per la qualificazione dei Cloud Service Provider per la PA" e n. 3 del 9 aprile 2018, recante i "Criteri per la qualificazione di servizi SaaS per il Cloud della PA";

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;

Esperita la procedura di informazione ai sensi della Direttiva (UE) n. 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 e della legge 21 giugno 1986 b, 317 modificata da ultimo dal decreto legislativo 15 dicembre 2017 n. 223, con comunicazione del 30 settembre 2021;

Considerata la trasmissione del testo del Regolamento al Garante per la protezione dei dati personali ai sensi dell'articolo 36, paragrafo 4, del regolamento (UE) n. 2016/679, in data 5 ottobre 2021;

Visti l'art. 154 commi 5 e 5bis del decreto legislativo 30 giugno 2003 n. 196 e l'articolo 9 del decreto legge 8 ottobre 2021 n.139 come convertito dalla legge 3 dicembre 2021 n. 205, con particolare riguardo al comma 1, lettere a) e i), e comma 7;

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 20212, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;
c) DTD, il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri;
d) D.L. 179/2012, 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) D.Lgs. 65/2018, 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";
f) D.L. 105/2019, 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";
g) Regolamento CSA, 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");
h) Amministrazioni centrali, le amministrazioni centrali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
i) Amministrazioni locali, le amministrazioni locali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;
j) Amministrazioni, le amministrazioni centrali di cui alla lettera h) e le amministrazioni locali di cui alla lettera i);
k) Dati dell'amministrazione, dati trattati tramite reti e sistemi informativi dell'amministrazione o tramite reti e sistemi informativi di terzi per conto dell'amministrazione;
l) Servizi dell'amministrazione, servizi erogati verso terzi o internamente all'amministrazione;
m) Servizi digitali dell'amministrazione, 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;
n) 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;

o) Infrastrutture digitali per le pubbliche amministrazioni, le infrastrutture digitali tramite le quali sono erogati i servizi digitali delle amministrazioni, ivi inclusi:
   - i CED, ovvero, ai sensi dall'articolo 33-septies, comma 2, del D.L. 179/2012, il sito che ospita 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;
   - l'infrastruttura promossa dalla Presidenza del Consiglio dei ministri di cui all'articolo 33-septies, comma 1, del D.L. 179/2012;
   - il polo strategico di cui all'articolo 33-septies, comma 4-ter, del D.L. 179/2012 realizzato dalla società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133 per l'attuazione e la conduzione dei progetti e la gestione dei dati, delle applicazioni e delle infrastrutture delle amministrazioni centrali di interesse nazionale previsti dal piano triennale per l'informatica nella pubblica amministrazione;
p) Servizi cloud, servizi informatici e risorse computazionali erogati su richiesta tramite internet da un fornitore, differenziati, sulla base del modello computazionale offerto, in tre categorie di servizi:
   - sistemistici infrastrutturali, c.d. Infrastructure-as-a-Service (IaaS), per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
   - 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;
   - 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;
q) Servizi cloud per la pubblica amministrazione, 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) Piano triennale per l'informatica nella pubblica amministrazione, il piano triennale di cui all'articolo 14-bis, comma 2, lett. b), del decreto legislativo 7 marzo 2005, n. 82;
t) Framework nazionale per la cybersecurity e la data protection, il Framework nazionale, edizione 2019, 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.

Articolo 2
(Finalità e oggetto)

1. Il presente Regolamento, in conformità alle previsioni di cui all'articolo 33-septies, comma 4, del D.L. 179/2012:
   a. stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione;

b. definisce le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione;
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. individua le modalità del procedimento di qualificazione dei servizi cloud per la pubblica amministrazione.

CAPO II
Elenco, caratterizzazione e classificazione dei dati e dei servizi della pubblica amministrazione

Articolo 3
(Elenco, caratterizzazione e classificazione dei dati e dei servizi)

1. Le amministrazioni predispongono e aggiornano un elenco dei loro dati e dei loro servizi digitali, comprensivo della descrizione delle relazioni:
   a. tra i dati e i servizi digitali dell'amministrazione;
   b. tra i dati e i servizi digitali dell'amministrazione e i dati e servizi di terzi.
2. I dati e i servizi digitali soggetti agli obblighi di cui al D.L. 105/2019 e di cui al D.Lgs. 65/2018 non sono oggetto dell'elencazione di cui al comma 1.
3. 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. strategici, se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale;
   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. ordinari, qualora la loro compromissione non determini i pregiudizi di cui alle lettere a) e b).
4. I dati e i servizi digitali soggetti agli obblighi di cui al D.L. 105/2019 sono classificati come strategici.
5. I dati e i servizi digitali soggetti agli obblighi di cui al D.Lgs. 65/2018 sono classificati come:
   a. strategici, qualora siano a valenza nazionale;
   b. critici, se non a valenza nazionale.

Articolo 4
(Modello per la predisposizione dell'elenco e della classificazione dei dati e dei servizi della pubblica amministrazione)

1. Entro il 18 gennaio 2022, l'ACN adotta, d'intesa con il DTD, un modello per la predisposizione e l'aggiornamento dell'elenco e della classificazione dei dati e dei servizi digitali di cui all'articolo 3 nonché le modalità di trasmissione.
2. Il modello di cui al comma 1 è elaborato:
   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.
3. Il modello di cui al comma 1 è reso disponibile tramite i canali di comunicazione dell'ACN ed è aggiornato su base periodica, almeno una volta ogni due anni, secondo le modalità di cui al medesimo comma.

Articolo 5

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

1. Entro il 18 luglio 2022, le amministrazioni trasmettono all'ACN l'elenco e la classificazione dei dati e dei servizi digitali di cui all'articolo 3 secondo il modello di cui all'articolo 4.
2. 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 stesse modalità di cui al precedente comma, in presenza di dati e servizi ulteriori rispetto a quelli già oggetto di conferimento e classificazione, nonché a seguito dell'aggiornamento del modello di cui all'articolo 4.
3. L'ACN fornisce riscontro circa la conformità dell'elenco e della classificazione dei dati e dei servizi di cui all'articolo 3 rispetto al modello di 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 conferimento dell'elenco e della classificazione dei dati e dei servizi della pubblica amministrazione.
4. 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 3 sono interrotti e ricominciano a decorrere dalla data di ricevimento delle informazioni che sono rese entro il termine di trenta giorni dalla richiesta.
5. Al termine della verifica di conformità di cui al comma 3, l'ACN:
   a) convalida la conformità dell'elenco e della classificazione dei dati e dei servizi di cui all'articolo 3;
   b) convalida, con prescrizioni, la conformità dell'elenco e della classificazione dei dati e dei servizi di cui all'articolo 3;
   c) non convalida, fornendone le motivazioni, la conformità dell'elenco e della classificazione dei dati e dei servizi di cui all'articolo 3.
6. Nell'ipotesi di cui al comma 5, lettera b), l'amministrazione trasmette all'ACN, entro trenta giorni, l'adeguamento dell'elenco e della classificazione dei dati e dei servizi alle prescrizioni.
7. In assenza di riscontro da parte dell'ACN entro i termini di cui ai commi 3 e 4, l'elenco e la classificazione dei dati e dei servizi si intendono convalidati.

CAPO III
Livelli minimi delle infrastrutture digitali e caratteristiche dei servizi cloud per la pubblica amministrazione

Articolo 6
(Criteri per la definizione dei livelli minimi delle infrastrutture digitali e caratteristiche dei servizi cloud per la pubblica amministrazione)

1. I livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture digitali per la pubblica amministrazione, nonché le caratteristiche dei servizi cloud per la pubblica amministrazione, di cui agli articoli 7 e 8, sono resi disponibili tramite i canali di comunicazione dell'ACN;
2. I livelli minimi di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità delle infrastrutture digitali per la pubblica amministrazione, nonché le caratteristiche dei servizi cloud per la pubblica amministrazione, 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 europei progressivamente adottati ai sensi del Regolamento CSA;
d. tenuto conto degli standard nazionali, quali il Framework Nazionale, europei e internazionali.

Articolo 7
(Livelli minimi delle infrastrutture per la pubblica amministrazione)

1. Le infrastrutture digitali per la pubblica amministrazione rispettano i livelli minimi di base di sicurezza, di capacità elaborativa, di risparmio energetico e di affidabilità definiti nell'**allegato A**.
2. Le amministrazioni che, a seguito del censimento del patrimonio ICT della pubblica amministrazione effettuato dall'AgID, in conformità con quanto previsto dal Piano triennale e dalla Circolare AgID n. 1 del 2019, sono dotate di infrastrutture digitali classificate "A", adottano i livelli minimi di base di cui al comma 1 entro dodici mesi dall'entrata in vigore del presente regolamento.
3. Entro il 18 gennaio 2022, con atti successivi, l'ACN aggiorna, d'intesa con il DTD e sulla scorta di quanto previsto dall'articolo 6, comma 2, ulteriori livelli minimi di sicurezza, di capacità elaborativa e di affidabilità che le infrastrutture della pubblica amministrazione devono rispettare per trattare i dati e i servizi digitali:
    a. classificati quali ordinari ai sensi dell'articolo 3;
    b. classificati quali critici ai sensi dell'articolo 3;
    c. classificati quali strategici ai sensi dell'articolo 3.
4. Le amministrazioni, entro dodici mesi dall'adozione dei relativi atti da parte dell'ACN, adeguano i livelli minimi delle infrastrutture per la pubblica amministrazione a quelli di cui al comma 3.
5. Le infrastrutture della pubblica amministrazione che trattano dati ed erogano servizi digitali soggetti al D.L. 105/2019 rispettano le prescrizioni di cui al predetto decreto.

Articolo 8
(Caratteristiche dei servizi cloud per la pubblica amministrazione)

1. I servizi cloud per la pubblica amministrazione possiedono le caratteristiche di base di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità definite nell'**allegato B**.
2. Le caratteristiche dei servizi cloud per la pubblica amministrazione sono adeguate a quelle di cui al comma 1 entro dodici mesi dall'entrata in vigore del presente regolamento.
3. Entro il 18 gennaio 2022, con atti successivi l'ACN aggiorna, d'intesa con il DTD e sulla scorta di quanto previsto dall'articolo 6, comma 2, le caratteristiche di qualità, di sicurezza, di performance e di scalabilità dei servizi cloud per la pubblica amministrazione che possono trattare i dati e i servizi digitali:
    a. classificati quali ordinari ai sensi dell'articolo 3;
    b. classificati quali critici ai sensi dell'articolo 3;
    c. classificati quali strategici ai sensi dell'articolo 3.
4. Le caratteristiche dei servizi cloud per la pubblica amministrazione sono adeguate a quelle di cui al comma 3 entro dodici mesi dall'adozione dei relativi atti dell'ACN.

CAPO IV
Migrazione dei dati e dei servizi della pubblica amministrazione

Articolo 9

(Criteri per la migrazione dei dati e dei servizi 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, i dati e servizi digitali verso le infrastrutture digitali che rispettano, in relazione alla classificazione di cui all'articolo 3, i livelli minimi di cui all'articolo 7 ovvero verso i servizi cloud che rispettano le caratteristiche di cui all'articolo 8 e abbiano ottenuto la qualificazione ai sensi dell'articolo 13.
2. La migrazione dei dati e dei servizi digitali soggetti agli obblighi di cui al D.L. 105/2019 e al D.Lgs. 65/2018, ai sensi del comma 1, avviene nel rispetto delle previsioni dei suddetti decreti.
3. Con atti successivi, l'ACN può definire misure ulteriori o di raccordo tra le previsioni del presente regolamento e quelle del D.L. 105/2019 e del D.Lgs. 65/2018.

Articolo 10

(Termini e modalità per la migrazione dei dati e dei servizi della pubblica amministrazione)

1. Le amministrazioni, all'esito del processo di conferimento 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 DTD, d'intesa con l'ACN.
2. Il modello di cui al comma 1 è reso disponibile tramite i canali di comunicazione del DTD e dell'ACN e può essere aggiornato, qualora necessario, secondo le modalità del medesimo comma.
3. Le amministrazioni, anche ai fini della verifica degli obblighi previsti dall'articolo 33-septies del D.L. 179/2012, trasmettono i piani di migrazione al DTD e all'AgID, mediante una piattaforma dedicata messa a disposizione dallo stesso DTD, entro il 28 febbraio 2023.
4. Le amministrazioni completano le attività previste dal piano di migrazione, trasmesso ai sensi del comma 3, entro il 30 giugno 2026.
5. Il DTD, anche avvalendosi di AgID, verifica il piano di migrazione e riscontra la conformità dello stesso rispetto al modello di cui al comma 1 entro sessanta giorni dalla data della sua ricezione. Il predetto termine può essere prorogato dal DTD, 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 5 sono interrotti 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 5, il DTD:
   a) convalida il piano di migrazione;
   b) convalida, con prescrizioni, il piano di migrazione;
   c) non convalida, fornendone le motivazioni, il piano di migrazione.
8. Nell'ipotesi di cui al comma 7, lettera b), l'amministrazione trasmette al DTD, entro trenta giorni, l'adeguamento del piano di migrazione alle prescrizioni.
9. In assenza di riscontro da parte del DTD entro i termini di cui ai commi 5 e 6, il piano di migrazione si intende convalidato.

CAPO V

Articolo 11
(Requisiti di qualificazione dei servizi cloud per la pubblica amministrazione)

1. Entro il 18 gennaio 2022, con atti successivi l'ACN definisce, d'intesa con il DTD e tenuto conto di quanto previsto dall'articolo 8, i criteri per la qualificazione dei servizi cloud per la pubblica amministrazione per le seguenti quattro tipologie:
    a. qualificazione cloud di livello 1 (QC1);
    b. qualificazione cloud di livello 2 (QC2);
    c. qualificazione cloud di livello 3 (QC3);
    d. qualificazione cloud di livello 4 (QC4).
2. I criteri di cui al comma 1 sono resi disponibile tramite i canali di comunicazione dell'ACN e sono aggiornati su base periodica, almeno una volta ogni due anni, secondo le modalità di cui al medesimo comma
3. I criteri 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 europei progressivamente adottati ai sensi del Regolamento CSA.
4. I dati e i servizi digitali classificati, ai sensi dell'articolo 3, quali:
    a. ordinari possono essere erogati tramite servizi cloud qualificati nell'ambito delle tipologie di cui al comma 1, lettere a e b;
    b. critici possono essere erogati tramite servizi cloud qualificati nell'ambito delle tipologie di cui al comma 1, lettere b, c e d;
    c. strategici possono essere erogati tramite servizi cloud qualificati nell'ambito delle tipologie di cui al comma 1, lettere c e d;

Articolo 12
(Modalità di trasmissione della domanda di qualificazione dei servizi cloud)

1. L'ACN predispone le modalità per la trasmissione delle domande di qualificazione di servizi cloud, d'intesa con il DTD, con l'indicazione della documentazione e le informazioni necessarie.
2. Le modalità di cui al comma 1 sono rese disponibile tramite i canali di comunicazione dell'ACN.
3. Le informazioni necessarie includono, almeno:
    e. la tipologia di qualificazione richiesta di cui all'articolo 11;
    f. la descrizione del servizio cloud per il quale viene richiesta la qualificazione;
    g. l'indicazione dei requisiti posseduti ai fini della qualificazione richiesta e la relativa documentazione.
4. Le domande di qualificazione sono trasmesse, secondo le modalità di cui al comma 1, dal soggetto richiedente all'ACN.

Articolo 13
(Processo di qualificazione dei servizi cloud)

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 12, l'ACN verifica la conformità ai criteri di cui all'articolo 11 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, anche mediante accesso all'infrastruttura fisica e logica 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 venti giorni, prorogabili ulteriormente di venti giorni in casi di particolare complessità. Ove si renda necessario chiedere informazioni al soggetto richiedente la qualificazione, ivi inclusi quelle di cui al comma 2, il termine di cui al comma 1 è interrotto e ricomincia a decorrere dalla data di ricevimento delle informazioni, che sono rese entro il termine di dieci giorni dalla richiesta.
4. Al termine della verifica di conformità di cui al comma 1, l'ACN:
    e. rifiuta, fornendone le motivazioni, la qualificazione del servizio cloud;
    f. rilascia, con condizioni motivate, la qualificazione del servizio cloud, specificandone la durata;
    g. rilascia, senza condizioni, la qualificazione del servizio cloud, specificandone la durata.
5. La qualificazione del servizio cloud ha una durata massima fino a due anni.
6. Entro 15 giorni dal termine della verifica di conformità di cui al comma 1, l'ACN ne comunica l'esito al soggetto richiedente e, contestualmente, nel caso di rilascio della qualificazione, pubblica la scheda del servizio in un catalogo reso disponibile tramite i canali di comunicazione dell'ACN.
7. Qualora emergano elementi di criticità relativi ai requisiti di qualificazione di cui all'articolo 11, l'ACN può revocare la qualificazione precedentemente rilasciata. I contratti stipulati dalle amministrazioni e aventi ad oggetto la fornitura di un servizio cloud per il quale è stata revocata la qualificazione precedentemente rilasciata sono risolti di diritto a decorrere dalla data di notifica del provvedimento di revoca.

Art. 14

(Entrata in vigore)

1. Il Regolamento adottato con la presente determinazione entrerà in vigore al termine del periodo di status quo conseguente alla notifica alla Commissione europea ai sensi della Direttiva (UE) n. 2015/1535.
2. Fino all'entrata in vigore dei decreti del Presidente del Consiglio dei Ministri di cui all'art. 17, c. 5, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, legge 4 agosto 2021, n. 109, restano ferme le attività per la qualificazione dei servizi cloud delle pubbliche amministrazioni svolte da AgID.

ALLEGATO A

Livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per la Pubblica Amministrazione

1. Livelli minimi di sicurezza e affidabilità

I livelli minimi di sicurezza e affidabilità sono definiti sulla base di:

- sotto-categorie del Framework Nazionale per la Cybersecurity e la Data Protection (di seguito FNCS). Per l'implementazione delle sotto-categorie è sufficiente la conformità ai relativi controlli/misure di uno tra gli standard e le regole tecniche riportati nelle *informative references* del FNCS;
- Allegato A della Circolare AgID 1 del 14 giugno 2019.

CODICE PROGRESSIVO (ID REQUISITO)	NOME	SPECIFICA REQUISITO
IN-SA-ID.AM-1-01	**Censimento apparati fisici**	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FNCS.
IN-SA-ID.AM-2-01	**Censimento piattaforme e applicazioni software**	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS.
IN-SA-ID.AM-3-01	**Censimento dei flussi di dati e delle comunicazioni**	L'Amministrazione implementa la sotto-categoria ID.AM-3 del FNCS.
IN-SA-ID.AM-6-01	**Ruoli e responsabilità inerenti alla cybersecurity**	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FNCS.
IN-SA-ID.GV-1-01	**Policy di cybersecurity**	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	**Identificazione delle vulnerabilità**	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FNCS.
IN-SA-ID.RA-5-01	**Valutazione del rischio**	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FNCS.

IN-SA-PR.AC-1-01	**Identity Management**	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FNCS.
IN-SA-PR.AC-2-01	**Controllo degli accessi fisici**	L'Amministrazione implementa la sotto-categoria PR.AC-2 del FNCS.
IN-SA-PR.AC-3-01	**Controllo degli accessi remoti**	L'Amministrazione implementa la sotto-categoria PR.AC-3 del FNCS.
IN-SA-PR.AC-4-01	**Privilegio minimo e separazione delle funzioni**	L'Amministrazione implementa la sotto-categoria PR.AC-4 del FNCS.
IN-SA-PR.AT-1-01	**Formazione e addestramento degli utenti**	L'Amministrazione implementa la sotto-categoria PR.AT-1 del FNCS.
IN-SA-PR.AT-2-01	**Ruolo e responsabilità degli utenti privilegiati**	L'Amministrazione implementa la sotto-categoria PR.AT-2 del FNCS.
IN-SA-PR.DS-1-01	**Localizzazione dei dati**	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
IN-SA-PR.DS-5-01	**Protezione contro l'esfiltrazione dei dati**	L'Amministrazione implementa la sotto-categoria PR.DS-5 del FNCS.
IN-SA-PR.DS-6-01	**Integrità dei dati**	L'Amministrazione implementa la sotto-categoria PR.DS-6 del FNCS.
IN-SA-PR.IP-1-01	**Baseline per la configurazione dei sistemi**	L'Amministrazione implementa la sotto-categoria PR.IP-1 del FNCS.
IN-SA-PR.IP-4-01	**Backup**	L'Amministrazione implementa la sotto-categoria PR.IP-4 del FNCS.

IN-SA-PR.IP-9-01	**Business continuity e Disaster recovery**	L'Amministrazione implementa la sotto-categoria PR.IP-9 del FNCS. E' stato predisposto il piano di Disaster recovery. Sono state adottate formali procedure di emergenza in caso di indisponibilità parziale dei servizi.
IN-SA-PR.IP-12-01	**Piano di gestione delle vulnerabilità**	L'Amministrazione implementa la sotto-categoria PR.IP-12 del FNCS.
IN-SA-PR.MA-1-01	**Manutenzione e riparazione dei sistemi**	L'Amministrazione implementa la sotto-categoria PR.MA-1 del FNCS.
IN-SA-PR.MA-2-01	**Manutenzione remota**	L'Amministrazione implementa la sotto-categoria PR.MA-2 del FNCS.
IN-SA-DE.CM-1-01	**Monitoraggio della rete**	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS.
IN-SA-DE.CM-4-01	**Rilevazione del codice malevolo**	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS.
IN-SA-DE.CM-7-01	**Monitoraggio del personale, delle connessioni, dei dispositivi e del software**	L'Amministrazione implementa la sotto-categoria DE.CM-7 del FNCS.
IN-SA-DE.CM-8-01	**Scansione delle vulnerabilità**	L'Amministrazione implementa la sotto-categoria DE.CM-8 del FNCS.
IN-SA-RS.MI-3-01	**Mitigazione vulnerabilità**	L'Amministrazione implementa la sotto-categoria RS.MI-3 del FNCS.
IN-SA-RC.RP-1-01	**Piano di ripristino**	L'Amministrazione implementa la sotto-categoria RC.RP-1 del FNCS.
IN-SA-DC-01-01	**Data center – presidio operativo**	L'Amministrazione garantisce il presidio operativo del Data Center 24/7/365.
IN-SA-DC-02-01	**Data center – titoli di possesso dei locali**	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: 1. Proprietà; 2.

		locazione/comodato da altra PA o Demanio; 3. leasing immobiliare con possibilità di riscatto; 4. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".
IN-SA-DC-03-01	**Data center – standard di progettazione**	Il Data Center deve essere stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.
IN-SA-DC-04-01	**Data center – pavimenti flottanti**	Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
IN-SA-DC-05-01	**Data center – disponibilità**	L'indice di disponibilità del singolo Data Center deve essere almeno pari al 99,98 % (come rapporto tra le ore totali di servizio del Data center e le ore di disponibilità del Data center) al netto dei fermi programmati e almeno pari al 99,6% comprendendo i fermi programmati.
IN-SA-DC-06-01	**Data center - antincendio**	L'Amministrazione deve garantire le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
IN-SA-DC-07-01	**Data center – continuità elettrica**	L'Amministrazione deve garantire che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
IN-SA-DC-08-01	**Data center – sistema di raffreddamento**	L'Amministrazione deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.

2. Livelli minimi di capacità elaborativa

CODICE PROGRESSIVO	NOME	SPECIFICA REQUISITO

(ID REQUISITO)		
IN-CE-01	**Catalogo dei servizi erogati dalla PA**	L'Amministrazione che eroga servizi ad altre amministrazioni deve formalizzare e pubblicare le informazioni relative ai servizi tramite il CED ricorrendo ad un apposito catalogo servizi, in conformità alle best practice ITIL. Il catalogo deve essere gestito e manutenuto attraverso un processo aderente alle best practice sul service catalogue management ITIL o alle linee guida riportate dallo standard ISO/IEC 20000-2.
IN-CE-02	**Trasparenza della Capacità di elaborazione IT**	L'Amministrazione che eroga servizi ad altre amministrazioni deve rendere nota la capacità di elaborazione totale del CED, quella occupata, quella libera per soddisfare i propri piani di capacity e quella a disposizione di Amministrazioni ospitate. Nello specifico, per ciascuna misura, l'Amministrazione deve dichiarare: - la superficie della sala CED o l'equivalente in numero di rack o di unità rack (U); - il numero e la tipologia di server fisici o di server farm disponibili, fornendo la capacità computazionale totale ottenuta come somma di memoria RAM disponibile [in GB], somma di CPU/Core e vCore, MIPs per gli apparati Mainframe, storage [in TB].
IN-CE-03	**Gestione e pubblicazione della capacità di elaborazione**	La capacità elaborativa del CED deve essere gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.

3. Livelli minimi di risparmio energetico

CODICE PROGRESSIVO (ID REQUISITO)	NOME	SPECIFICA REQUISITO
IN-RE-01	**Efficienza Energetica**	L'Amministrazione deve determinare con frequenza annuale l'efficienza energetica del proprio 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 del DC e quella sostenuta per gli apparati.
IN-RE-02	**Gestione energetica ed ambientale**	L'Amministrazione deve avere adottato formalmente procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)

ALLEGATO B

Caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione

1. Caratteristiche di qualità

CODICE PROGRESSIVO (ID REQUISITO)	NOME	SPECIFICA REQUISITO
SC-QU-01	**Qualità aziendale**	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione della qualità in conformità allo standard ISO/IEC 9001.
SC-QU-02	**Gestione dei servizi IT**	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione dei servizi IT in conformità allo standard ISO/IEC 20000.
SC-QU-03	**Attività di supporto**	Per il servizio cloud devono essere garantite attività di supporto ai clienti. Il servizio di supporto deve essere: (I) fornito esclusivamente in lingua italiana durante le business hours, anche in lingua inglese per le emergenze 24/7; (II) accessibile almeno tramite uno dei seguenti canali preferenziali: recapito telefonico ed e-mail. In aggiunta, deve essere messo a disposizione dell'Amministrazione Acquirente un sistema di troubleshooting, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i casi di supporto.

2. Caratteristiche di sicurezza

Le caratteristiche minime di sicurezza sono definite sulla base delle sotto-categorie del Framework Nazionale per la Cybersecurity e la Data Protection (di seguito FNCS). Per l'implementazione delle sotto-categorie è sufficiente la conformità ai relativi controlli/misure di uno tra gli standard e le regole tecniche riportati nelle informative references del FNCS.

CODICE PROGRESSIVO (ID REQUISITO)	NOME	SPECIFICA REQUISITO

SC-SI-ID.AM-1-01	**Censimento apparati fisici**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-1 del FNCS.
SC-SI-ID.AM-2-01	**Censimento piattaforme e applicazioni software**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-2 del FNCS.
SC-SI-ID.AM-3-01	**Censimento dei flussi di dati e delle comunicazioni**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-3 del FNCS.
SC-SI-ID.AM-6-01	**Ruoli e responsabilità inerenti alla cybersecurity**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-6 del FNCS.
SC-SI-ID.RA-1-01	**Identificazione delle vulnerabilità**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-1 del FNCS.
SC-SI-ID.RA-5-01	**Valutazione del rischio**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-5 del FNCS.
SC-SI-PR.AC-1-01	**Identity Management**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-1 del FNCS.
SC-SI-PR.AC-2-01	**Controllo degli accessi fisici**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-2 del FNCS.
SC-SI-PR.AC-3-01	**Controllo degli accessi remoti**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-3 del FNCS.
SC-SI-PR.AC-4-01	**Privilegio minimo e separazione delle funzioni**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-4 del FNCS.
SC-SI-PR.AT-1-01	**Formazione e addestramento degli utenti**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-1 del FNCS.
SC-SI-PR.AT-2-01	**Ruolo e responsabilità degli utenti privilegiati**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-2 del FNCS.
SC-SI-PR.DS-1-01	**Localizzazione dei dati**	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.

SC-SI-PR.DS-5-01	**Protezione contro l'esfiltrazione dei dati**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-5 del FNCS.
SC-SI-PR.DS-6-01	**Integrità dei dati**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-6 del FNCS.
SC-SI-PR.IP-1-01	**Baseline per la configurazione dei sistemi**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-1 del FNCS.
SC-SI-PR.IP-4-01	**Backup**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-4 del FNCS.
SC-SI-PR.IP-9-01	**Business continuity e Disaster recovery**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-9 del FNCS.
SC-SI-PR.IP-12-01	**Piano di gestione delle vulnerabilità**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-12 del FNCS.
SC-SI-PR.MA-1-01	**Manutenzione e riparazione dei sistemi**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-1 del FNCS.
SC-SI-PR.MA-2-01	**Manutenzione remota**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-2 del FNCS.
SC-SI-DE.CM-1-01	**Monitoraggio della rete**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS.
SC-SI-DE.CM-4-01	**Rilevazione del codice malevolo**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS.
SC-SI-DE.CM-7-01	**Monitoraggio del personale, delle connessioni, dei dispositivi e del software**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-7 del FNCS.
SC-SI-DE.CM-8-01	**Scansione delle vulnerabilità**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-8 del FNCS.
SC-SI-RS.MI-3-01	**Mitigazione vulnerabilità**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RS.MI-3 del FNCS.
SC-SI-RC.RP-1-01	**Piano di ripristino**	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RC.RP-1 del FNCS.

3. Caratteristiche di performance e scalabilità

CODICE PROGRESSIVO (ID REQUISITO)	**NOME**	**SPECIFICA REQUISITO**

SC-PS-01	**Caratteristiche del servizio cloud**	Il servizio cloud deve garantire le seguenti caratteristiche come da indicazioni NIST SP 800-145 e ISO/IEC 17788:2014: 1) Self-Service provisioning: all'utente deve essere garantito di poter provvedere alla fornitura delle risorse informatiche secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Le richieste di risorse computazionali inerenti al servizio cloud oggetto di qualificazione (o informatiche) devono essere fornite unilateralmente, senza la verifica o l'approvazione del fornitore. 2) Accesso alla rete: per il servizio cloud oggetto di qualificazione devono essere offerte opzioni multiple di connettività alla rete e una di queste deve essere obbligatoriamente basata su rete pubblica (i.e. internet). 3) Pool di risorse: le risorse informatiche relative al servizio oggetto di qualificazione devono essere offerte in un pool, in modo da servire più utenti tramite un modello multi-tenant con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda degli utenti. 4) Elasticità rapida: deve essere supportato il provisioning e de-provisioning del servizio cloud oggetto di qualificazione. 5) Servizio misurabile: la fornitura a consumo del servizio cloud oggetto di qualificazione deve essere tale che l'utilizzo possa essere monitorato, controllato, segnalato e fatturato; 6) Multi-tenant: le risorse fisiche o virtuali relative al servizio oggetto di qualificazione devono essere allocate in modo tale che più tenant e relative computations e dati siano isolati e inaccessibili l'uno dall'altro.
SC-PS-02	**Meccanismi e modalità di scalabilità del servizio cloud**	In merito alla scalabilità del servizio cloud, devono essere gestiti e dichiarati i seguenti aspetti: - il meccanismo di scalabilità offerto (automatico e configurabile, nativo, manuale); - la tipologia (orizzontale e/o verticale); - condizione massime di carico sopportabili dal servizio (numero di utenti concorrenti e/o volume di richieste processabili); - le modalità di configurazione (sulla base di metriche di monitoraggio, pianificato nel tempo); - i tempi minimi di reazione del servizio alla richiesta di nuove risorse (i.e. attivazione di nuove risorse). In aggiunta, il fornitore rende disponibili 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.

4. Caratteristiche di interoperabilità e portabilità

CODICE PROGRESSIVO (ID REQUISITO)	NOME	SPECIFICA REQUISITO
SC-IP-01	**Presenza di API per la gestione automatica e remota del ciclo di vita dei servizi**	L'ambiente cloud del servizio deve essere accessibile tramite delle API per la gestione remota. Le API esposte devono consentire l'implementazione di automatismi per la gestione remota del ciclo di vita del servizio cloud qualificato. In aggiunta, deve essere prevista la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-02	**Conformità delle API al modello di interoperabilità AgID**	Per tutte le API esposte dal servizio cloud deve essere dichiarata l'eventuale conformità al Modello di interoperabilità emanato da AgID. Il Modello è descritto dalle linee guida riportate nella circolare AgID, n. 1 del 9 settembre 2020 e i relativi allegati, e dalle ssm. 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).
SC-IP-03	**Presenza di API per funzionalità applicative**	I servizi SaaS devono esporre opportune API di tipo SOAP e/o REST associate alle funzionalità applicative. Tali API devono prevedere la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-04	**Portabilità dei dati, utilizzo di formati open**	Il servizio cloud deve garantire la disponibilità di funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati garantendo l'utilizzo di formati open non proprietari.