Allegato 1

"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"

(articoli 7, 8, 11 del 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, adottato dall'Agenzia per l'Italia digitale ai sensi dell'articolo 17, comma 6, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)

Capo I
Disposizioni di carattere generale

Articolo 1
(Definizioni)

1. Ai fini del presente documento 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) DTD, il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri;

c) Regolamento, 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, recante "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", adottato dall'AgID con Determinazione n. 628/2021 del 15 dicembre 2021;

d) Amministrazioni centrali, le amministrazioni centrali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;

e) Amministrazioni locali, le amministrazioni locali individuate dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;

f) Amministrazioni, le amministrazioni centrali di cui alla lettera d) e le amministrazioni locali di cui alla lettera e);

g) Dati dell'amministrazione, dati trattati tramite reti e sistemi informativi dell'amministrazione o tramite reti e sistemi informativi di terzi per conto dell'amministrazione;

h) Servizi dell'amministrazione, servizi erogati verso terzi o internamente all'amministrazione;

i) 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;

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 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;
   2) l'infrastruttura promossa dalla Presidenza del Consiglio dei ministri di cui all'articolo 33-septies, comma 1, del D.L. 179/2012;

n) 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:
   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;

o) Servizio cloud per la pubblica amministrazione, un servizio cloud erogato da un fornitore ad una amministrazione tramite il quale sono erogati servizi digitali di quella amministrazione;

p) Compromissione, la compromissione di dati o servizi digitali in termini di confidenzialità, integrità o disponibilità;

q) Qualificazione dei servizi cloud, processo di verifica formale per garantire che i servizi cloud, e l'infrastruttura sottostante, di cui si avvalgono le amministrazioni, siano in possesso delle caratteristiche necessarie per trattare dati e servizi classificati quali ordinari, critici e strategici ai sensi dell'articolo 3 del Regolamento, assicurando, in particolare, opportuni livelli di qualità, di performance, di scalabilità, di portabilità, nonché di sicurezza;

r) 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. Fermo restando quanto previsto dal Regolamento, in conformità alle previsioni di cui agli articoli 7, 8 e 11 dello stesso Regolamento:
   a) sono aggiornati i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità che le infrastrutture per la pubblica amministrazione che possono trattare i dati e i servizi digitali classificati quali ordinari, critici e strategici ai sensi dell'articolo 3 del Regolamento;
   b) sono aggiornate le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione che possono trattare i dati e i servizi digitali classificati quali ordinari, critici e strategici ai sensi dell'articolo 3 del Regolamento;
   c) sono definiti i requisiti per la qualificazione dei servizi cloud per la pubblica amministrazione.

CAPO II
Livelli minimi per le infrastrutture per la pubblica amministrazione e caratteristiche dei servizi cloud per la pubblica amministrazione

Articolo 3
(Livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità per le infrastrutture per la pubblica amministrazione)

1. Fermo restando quanto previsto dall'allegato A al Regolamento, l'allegato A2 aggiorna gli ulteriori livelli minimi di sicurezza, di capacità elaborativa e di affidabilità delle infrastrutture della pubblica amministrazione di cui all'articolo 7, comma 3, del Regolamento. L'allegato A2 è suddiviso in sezioni recanti i livelli minimi per trattare i dati e i servizi digitali classificati quali ordinari, critici e strategici ai sensi dell'articolo 3 del Regolamento.
2. Per trattare i dati e i servizi digitali classificati quali ordinari ai sensi dell'articolo 3 del Regolamento, le infrastrutture della pubblica amministrazione devono rispettare i livelli minimi di cui alla sezione 2 dell'allegato A2.
3. Per trattare i dati e i servizi digitali classificati quali critici ai sensi dell'articolo 3 del Regolamento, le infrastrutture della pubblica amministrazione devono rispettare i livelli minimi di cui alle sezioni 2 e 3 dell'allegato A2.
4. Per trattare i dati e i servizi digitali classificati quali strategici ai sensi dell'articolo 3 del Regolamento, le infrastrutture della pubblica amministrazione devono rispettare i livelli minimi di cui alle sezioni 2, 3 e 4 dell'allegato A2.
5. Le amministrazioni, dopo l'avvenuta adozione dei livelli minimi di cui all'allegato A2 nei termini di cui all'articolo 7, comma 4, del Regolamento, ne danno tempestivamente comunicazione all'ACN, descrivendo le relative modalità.
6. Ai fini della comunicazione di cui al comma 5, l'ACN predispone un apposito modello reso disponibile tramite i propri canali di comunicazione.
7. Qualora una amministrazione realizzi modifiche sostanziali delle modalità di adozione dei livelli minimi di cui all'allegato A2, successivamente alla comunicazione di cui al comma 5, ne comunica, entro sei mesi, le relative modalità all'ACN con il modello di cui al comma 6.

Articolo 4
(Caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione)

1. Fermo restando quanto previsto dall'allegato B al Regolamento, l'allegato B2 aggiorna le ulteriori caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione di cui all'articolo 8, comma 3, del Regolamento. L'allegato B2 è suddiviso in sezioni recanti le caratteristiche per trattare i dati e i servizi digitali classificati quali ordinari, critici e strategici ai sensi dell'articolo 3 del Regolamento.
2. Per trattare i dati e i servizi digitali classificati quali ordinari ai sensi dell'articolo 3 del Regolamento, i servizi cloud per la pubblica amministrazione devono rispettare le caratteristiche di cui alla sezione 2 dell'allegato B2.
3. Per trattare i dati e i servizi digitali classificati quali critici ai sensi dell'articolo 3 del Regolamento, i servizi cloud per la pubblica amministrazione devono rispettare le caratteristiche di cui alle sezioni 2 e 3 dell'allegato B2.
4. Per trattare i dati e i servizi digitali classificati quali strategici ai sensi dell'articolo 3 del Regolamento, i servizi cloud per la pubblica amministrazione devono rispettare le caratteristiche di cui alle sezioni 2, 3 e 4 dell'allegato B2.
5. Le caratteristiche di cui ai commi 2, 3 e 4 sono adottate nei termini di cui all'articolo 8, comma 4, del Regolamento.

CAPO III
Qualificazione dei servizi cloud per la pubblica amministrazione

Articolo 5
(Catena di qualificazione dei servizi cloud)

1. I servizi cloud di cui all'articolo 1, comma 1, lettera *n)*, erogati, in ultima istanza, da un'infrastruttura del servizio cloud, sono suddivisi in tre categorie di servizi:
   a) sistemistici infrastrutturali, c.d. Infrastructure-as-a-Service (IaaS): categoria di servizi cloud in cui le funzionalità offerte sono di tipo infrastrutturale. Tali funzionalità consentono al fruitore del servizio di disporre autonomamente in modo programmatico di risorse infrastrutturali (quali, ad esempio, risorse computazionali, spazio di salvataggio dati e funzionalità di rete). Un servizio cloud di tipo Infrastructure-as-a-Service (IaaS) viene erogato tramite l'infrastruttura del servizio cloud;
   b) piattaforme computazionali, c.d. Platform-as-a-Service (PaaS): categoria di servizi cloud in cui le funzionalità offerte sono di tipo programmatico, ovvero il fruitore del servizio può amministrare, dispiegare ed eseguire applicazioni utilizzando uno o più linguaggi di programmazione, uno o più ambienti di sviluppo o esecuzione supportati dal servizio cloud e i relativi componenti software a corredo (quali, ad esempio, code di messaggi, database). Un servizio cloud di tipo Platform-as-a-Service (PaaS) viene erogato tramite un servizio cloud di tipo Infrastructure-as-a-Service (IaaS) o direttamente tramite l'infrastruttura del servizio cloud;
   c) applicativi, c.d. Software-as-a-Service (SaaS): categoria di servizi interamente gestiti dal soggetto che eroga il servizio cloud, gestendo la predisposizione, la configurazione, la messa in esercizio e la manutenzione del servizio cloud stesso, lasciando all'amministrazione il solo ruolo di utilizzatore finale delle funzionalità offerte. Un servizio cloud di tipo Software-as-a-Service (SaaS) viene erogato tramite un servizio cloud di tipo Infrastructure-as-a-Service (IaaS), o di tipo Platform-as-a-Service (PaaS), o direttamente tramite l'infrastruttura del servizio cloud.
2. I livelli di qualificazione di cui all'articolo 11 del Regolamento sono definiti su quattro livelli crescenti, nel seguente ordine:

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).

3. Al fine di ottenere una delle qualificazioni di cui all'articolo 11 del Regolamento per uno specifico livello, un servizio cloud di tipo Infrastructure-as-a-Service (IaaS) deve essere erogato tramite un'infrastruttura qualificata, ai sensi dell'articolo 7, per il livello medesimo o superiore.
4. Al fine di ottenere una delle qualificazioni di cui all'articolo 11 del Regolamento per uno specifico livello, un servizio cloud di tipo Platform-as-a-Service (PaaS) deve essere erogato tramite:
   a) un servizio Infrastructure-as-a-Service (IaaS) qualificato per il livello medesimo o superiore;
   b) ovvero, qualora non sia erogato tramite un servizio Infrastructure-as-a-Service (IaaS), un'infrastruttura qualificata, ai sensi dell'articolo 7, per il livello medesimo o superiore.
5. Al fine di ottenere una delle qualificazioni di cui all'articolo 11 del Regolamento per uno specifico livello, un servizio cloud di tipo Software-as-a-Service (SaaS) deve essere erogato tramite:
   a) un servizio Platform-as-a-Service (PaaS) qualificato per il livello medesimo o superiore; ovvero
   b) qualora non sia erogato tramite un servizio Platform-as-a-Service (PaaS), un servizio Infrastructure-as-a-Service (IaaS) qualificato per il livello medesimo o superiore; ovvero
   c) qualora non sia erogato tramite un servizio Platform-as-a-Service (PaaS) o Infrastructure-as-a-Service (IaaS), un'infrastruttura qualificata, ai sensi dell'articolo 7, per il livello medesimo o superiore.

Articolo 6
(Definizione dei requisiti di qualificazione dei servizi cloud)

1. I requisiti per la qualificazione dei servizi cloud sono individuati nell'allegato C. I requisiti di qualificazione per ogni livello di qualificazione sono elencati in una sezione dedicata dell'allegato C, secondo quanto indicato ai commi 2, 3, 4 e 5.
2. Per ottenere la qualificazione di livello 1 (QC1) di cui all'articolo 11 del Regolamento, il servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 2 dell'allegato C.
3. Per ottenere la qualificazione di livello 2 (QC2) di cui all'articolo 11 del Regolamento, il servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 3 dell'allegato C.
4. Per ottenere la qualificazione di livello 3 (QC3) di cui all'articolo 11 del Regolamento, il servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 4 dell'allegato C.
5. Per ottenere la qualificazione di livello 4 (QC4) di cui all'articolo 11 del Regolamento, il servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 5 dell'allegato C.

Articolo 7
(Livelli di qualificazione delle infrastrutture dei servizi cloud)

1. I requisiti per la qualificazione delle infrastrutture dei servizi cloud per la pubblica amministrazione, definiti ai sensi dell'articolo 8, sono suddivisi nei seguenti quattro livelli, elencati dalla qualificazione meno stringente a quella più stringente:
   a) qualificazione infrastruttura di livello 1 (QI1);
   b) qualificazione infrastruttura di livello 2 (QI2);
   c) qualificazione infrastruttura di livello 3 (QI3);
   d) qualificazione infrastruttura di livello 4 (QI4).

Articolo 8
(Definizione dei requisiti di qualificazione delle infrastrutture dei servizi cloud)

1. I requisiti per la qualificazione delle infrastrutture dei servizi cloud di cui all'articolo 7 sono individuati nell'allegato C. I requisiti di qualificazione per ogni livello di qualificazione sono elencati in una sezione dedicata dell'allegato C, secondo quanto indicato ai commi 2, 3, 4 e 5.
2. Per ottenere la qualificazione di livello 1 (QI1) di cui all'articolo 7, l'infrastruttura del servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 6 dell'allegato C.
3. Per ottenere la qualificazione di livello 2 (QI2) di cui all'articolo 5, l'infrastruttura del servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 7 dell'allegato C.
4. Per ottenere la qualificazione di livello 3 (QI3) di cui all'articolo 5, l'infrastruttura del servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 8 dell'allegato C.
5. Per ottenere la qualificazione di livello 4 (QI4) di cui all'articolo 5, l'infrastruttura del servizio cloud deve rispettare i requisiti di qualificazione elencati nella sezione 9 dell'allegato C.

Allegato A2 - Livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per la Pubblica Amministrazione

Gennaio 2022, versione 1.0

1. PREMESSA

1. Il presente allegato definisce le caratteristiche di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per la Pubblica Amministrazione di cui all'art. 7 c. 1 del Regolamento, che possono ospitare, rispettivamente, servizi e dati digitali della PA classificati, ai sensi del processo di cui all'art. 5 del Regolamento, quali ordinari, critici o strategici.

2. Le caratteristiche di sicurezza 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.

Sono, altresì, indicate raccomandazioni, la cui attuazione è demandata alle valutazioni di ciascun soggetto.

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

4. Ai fini del presente allegato, si intende per:

a. **Regolamento**, 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, recante "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", adottato dall' AgID con Determinazione n. 628/2021 del 15 dicembre 2021;

b. **Infrastruttura digitale,** le infrastrutture digitali per la Pubblica Amministrazione di cui all'art.1 co.1 lett. o del Regolamento**.**

c. **Soggetto**, il soggetto che detiene l'infrastruttura digitale;

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 soggetto, da cui dipende il funzionamento dell'infrastruttura digitale;

f. **Catena di approvvigionamento *cyber***, la catena di approvvigionamento relativa all'infrastruttura digitale.

2. ORDINARI

2.1. Affidabilità

2.1.1. Alta affidabilità

A.AA-1: Disponibilità dell'infrastruttura
1. L'indice di disponibilità dell'Infrastruttura Digitale deve essere stato almeno pari al valore di riferimento corrispondente per il servizio (SL1) così come indicato in Tabella 1 "Indicatori minimi di Servizio dell'infrastruttura".

A.AA-2 : Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità
1. 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. Governance e processi

A.GP-1: I Servizi IT sono gestiti conformemente agli standard di settore
1. Sono adottati processi e procedure in linea con le *best practice* indicate dalla ISO/IEC 20000-2.

A.GP-2: È garantito il rispetto degli indicatori di servizio obbligatori
1. Il soggetto deve garantire per i servizi del Centro di elaborazione dati (CED) offerti attività di supporto in conformità con gli obiettivi (SLO) identificati per i corrispondenti indicatori di servizio (SLI) riportati nella Tabella 1.
2. Il servizio di supporto deve essere:
   a. fornito esclusivamente in lingua italiana durante le business hours
   b. accessibile preferenzialmente tramite i seguenti canali: recapito telefonico ed e-mail.

2.1.3.

2.1.4. Performance e scalabilità

A.PS-1: Sono garantite caratteristiche minime di connettività
1. 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: *bandwidth* di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.

2.2. Sicurezza

IDENTIFY (ID)

2.2.1. 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-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione
1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. 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-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati
1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi all'Infrastruttura digitale, sono identificati e approvati da attori interni al soggetto.

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. È nominato, nell'ambito dell'articolazione di cui al punto 1, 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. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, 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.
4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.

2.2.2. 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-1: È identificata e resa nota una policy di cybersecurity
1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.

2.2.3. 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-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dell'Infrastruttura digitale e dell'efficacia delle misure di sicurezza tecniche e procedurali che contiene, inoltre, la periodicità e le modalità di esecuzione.
2. 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-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
1. 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. L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale.
3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.

PROTECT (PR)

2.2.4. 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-1: 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. 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.

2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.
3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).
5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.

PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato
1. Con riferimento ai censimenti della sottocategoria ID.AM-1, esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi.

PR.AC-3: L'accesso remoto alle risorse è amministrato
1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.
2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzati degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.
3. 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. Esiste un log degli accessi eseguiti da remoto.

PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
1. 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. 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. Sono definite e implementate politiche e procedure, 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.

2.2.5. 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-1: Il personale del soggetto è informato e addestrato
1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personal del soggetto e le modalità di verifica dell'acquisizione dei contenuti.
2. L'addestramento e la formazione di cui al punto 1 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;
   d. la definizione di ruoli e delle responsabilità;
   e. politiche di accesso a sistemi, asset e risorse;
   f. politiche di gestione delle informazioni e della sicurezza;
   g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;
   h. requisiti per la non divulgazione/confidenzialità di informazioni.

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

1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.

2.2.6. 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-1: I dati memorizzati sono protetti
1.Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
2. Con riferimento alle infrastrutture, al trattamento dei dati e dei servizi dell'Amministrazione, resta fermo quanto previsto dall'allegato A al Regolamento, requisito IN-SA-PR.DS-1-01.
3. 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.

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
1. 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. Sono adottate politiche di *Data Loss Prevention* coerentemente con la valutazione dei rischi.

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

2.2.7. 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 assets.

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
1. 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-4: I backup delle informazioni sono eseguiti, amministrati e verificati
1. Viene effettuato periodicamente un *backup* dei dati memorizzati. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup.
2. Viene verificato periodicamente il ripristino (test di *restore*) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"

PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità
1. Esiste un documento aggiornato di dettaglio che indica almeno:

a. le politiche di sicurezza adottate per gestire le vulnerabilità;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. 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.

2.2.8. 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-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.
2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.

DETECT (DE)

2.2.9. 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-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
1. Sono presenti sistemi di rilevamento delle intrusioni (*Intrusion Detection Systems* - IDS).
2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.

DE.CM-4: Il codice malevolo viene rilevato
1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (*Endpoint Protection Systems* - EPS)
2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.

DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità
1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti *penetration test* e *vulnerability assessment*, prima della loro messa in esercizio.
2. Sono eseguiti periodicamente *penetration test* e *vulnerability assessment* in relazione alla criticità delle piattaforme e delle applicazioni software.
3. Esiste un documento aggiornato recante la tipologia di *penetration test* e *vulnerability assessment* previsti.
4. Esiste un registro aggiornato dei *penetration test* e *vulnerability assessment* eseguiti corredato dalla relativa documentazione.

RESPOND (RS)

2.2.10. 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-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.
2. 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)

2.2.11. 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-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.

2.3. Data Center Security

S.DC-01: I Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale
1. Il soggetto garantisce il presidio operativo del Data Center 24/7/365.
2. 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. Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
4. Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
5. 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. 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. 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. 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.Capacità elaborativa

CE.CE-01: Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore
1. 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.

2.5.Risparmio energetico

RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore
1. Il soggetto ha formalmente adottato 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).

RE-GE-02: Valutazione annuale dell'efficienza energetica del Data Center
1. Il soggetto determina 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.

3. CRITICI

3.1. Sicurezza

3.1.1. 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-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione
1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.
2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate.
3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché gestione non autorizzata degli asset dell'organizzazione.

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
5. 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.
6. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 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.
7. L'incaricato di cui al punto 2 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 82/2021, e alle attività di verifica e ispezione

IDENTIFY (ID)

3.1.2. 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-1: È identificata e resa nota una policy di cybersecurity
2. Il Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.

ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity
1. 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.

3.1.3. 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-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
4. 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 digitale, opportunamente descritti e valutati;
   d. l'identificazione, l'analisi e la ponderazione del rischio

3.1.4. 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-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
1. Esiste un documento aggiornato di dettaglio che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

PROTECT (PR)

3.1.5. 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-1: 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. 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, 2, 3, 4, 5, 6,
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-2: L'accesso fisico alle risorse è protetto e amministrato

3. E' definito un perimetro di sicurezza tra le aree amministrative e le aree di *data storage* e *processing*.

PR.AC-3: L'accesso remoto alle risorse è amministrato
5. 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-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.
2. 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-7: 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. 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.

3.1.6. 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-2: I dati sono protetti durante la trasmissione
1. 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-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
1. 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-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
1. 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.

3.1.7. 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 assets.

PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni
1. 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. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione
3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.

PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati
3. 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-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro 1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi l'Infrastruttura digitale.
2. 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. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
4. I piani di *business continuity* sono collaudati e comunicati alle parti interessate.
5. La documentazione di cui al punto 2 è resa disponibile all'Amministrazione e rivista periodicamente.
6. L'impatto derivante da interruzioni ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.

3.1.8. 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-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
1. 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-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.

3.1.9. 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-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. 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-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
1. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
   a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;
2. Esistono meccanismi per garantire la continuità operativa, nel rispetto delle misure di sicurezza qui elencate.
3. Sono definite:
   a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DETECT (DE)

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

DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
1. Ai fini di rilevare tempestivamente incidenti con impatto dell'infrastruttura, 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 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), b) e c), per rilevare tempestivamente eventi di interesse.
2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi.
3. Sono definite:
   a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a);
   b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b);
   c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c).
   d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.
4. 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. 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. 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.

3.1.11. 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-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati
1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati.
2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete.
3. Gli strumenti tecnici di cui ai punti 1 e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.
4. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability
1. Le nomine di cui alla sottocategoria ID-AM-6 sono rese note all'interno del soggetto.
2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. i ruoli, i processi e le responsabilità di cui al punto 2;
   b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.
4. 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)

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

RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE, nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria al CSIRT Italia, degli incidenti con impatto sull'Infrastruttura digitale.

3.1.14. 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-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente
1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.
2. Sono eseguite periodicamente esercitazioni.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2;
   b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2;
   c. le modalità per le esercitazioni di cui al punto 3.

RS.CO-5: 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 awareness)
1. Sono definiti e mantenuti contatti con gruppi di interesse legati all'infrastruttura digitale e altre entità rilevanti e in linea con il contesto del soggetto in relazione all'infrastruttura digitale.

2. 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.

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

RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)
1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei *penetration test* e *vulnerability assessment* di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto.
2. 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. Esiste un documento aggiornato che descrive, almeno:
   a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2;
   b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.

RECOVER (RC)

3.1.16. 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-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
2. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

3.2.Datacenter Security

A.DC-1: La progettazione/realizzazione del Data Center garantisce la manutenibilità a caldo, conformemente agli standard di mercato.
1. 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 2.

3.3.Affidabilità

3.3.1. Business Continuity e Disaster Recovery

A.BC-3: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti
1. Provider di infrastruttura: L'infrastruttura digitale è dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 12 ore e RPO 12 ore.
2. Public Cloud provider: devono essere presenti servizi cloud di Disaster Recovery.

4.STRATEGICI

4.1.Sicurezza

IDENTIFY (ID)

4.1.1. 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-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
8. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).

4.1.2. 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-1: È identificata e resa nota una policy di cybersecurity
3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato.
4. 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

4.1.3. 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-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
3. 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. Esiste un documento per la correzione delle vulnerabilità che prevede anche la notifica alle parti interessate.

4.1.4. 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-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (*Shared Security Responsibility Model-SSRM*) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale.
4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi incluse le Infrastrutture digitali.

ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber
1. In merito all'affidamento di forniture sono adottate misure in materia di sicurezza della catena di approvvigionamento attraverso:
   a. il coinvolgimento dell'organizzazione di cybersecurity, tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione;
   b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore;
   c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza 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:

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

2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per il funzionamento dell'infrastruttura, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1 lettera d..
3. Si raccomanda, ove possibile e in relazione alla criticità di:
a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto:
i. della disponibilità del fornitore a condividere il codice sorgente;
ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore;
iii. 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*;
iv. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato e eseguito.
b. adottare processi e strumenti tecnici per:
i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore;
ii. acquisire il codice oggetto dai beni e sistemi di *Information and Communication Technology*;
iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito.

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

ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali
1. Esiste un documento aggiornato 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. 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. 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.Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.
5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di Remediation.

PROTECT (PR)

4.1.5. 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-3: L'accesso remoto alle risorse è amministrato
6. Le politiche e procedure aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, del soggetto.
7. È definito ed implementato un processo di autorizzazione congiunta con l'Amministrazione nel caso in cui vengano effettuati accessi ai dati della stessa. Nel caso in cui ciò non fosse possibile, il soggetto contatta l'Amministrazione nel minor tempo possibile informandolo degli accessi effettuati.
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-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

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

3. Con riferimento ai censimenti di cui alla categoria ID.AM, esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti;
   b. la descrizione delle reti segregate/segmentate;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza;
   d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.

PR.AC-7: 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. 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.

4.1.6. 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-1: Il personale del soggetto è informato e addestrato
3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.

PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità
3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2

4.1.7. 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-1: I dati memorizzati sono protetti
4. 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.

PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti.
3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto.
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

4.1.8. 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 assets.

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
2. 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. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni.
4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità
5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni vulnerabilità delle applicazioni, automatizzando la riparazione quando possibile.
6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni.
7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, *patching* e/o applicazioni

PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.IP-9: Sono attivi ed amministrati piani di recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.
7. 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. 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. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
10. Le strategie di *disaster recovery* sono collaudate e comunicate alle parti interessate.
11. 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. 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. 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
2. Il documento di cui al punto 1 della misura PR.IP-12 dovrà essere aggiornato su base semestrale.
3. 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.*

4.1.9. 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-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
2. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.
3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
4. 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. In base all'analisi del rischio di cui alla misura ID.RA-5, 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. Gli aggiornamenti software devono essere consentiti solo da fonti pre-autorizzate.
7. 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. Esiste un documento aggiornato che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 5, 6 e 7.

PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
6. Esiste un documento aggiornato di dettaglio che descrive, almeno, i processi e gli strumenti tecnici impiegati per realizzare i punti 2, 3, 4 e 5.

4.1.10. 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-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

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

PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
1-bis. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
a. sono adottate architettura ridondate di rete, di connettività, nonché applicative.
b. esiste un sito di *disaster recovery*.
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3.

DETECT (DE)

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

DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
10. Esiste una *repository* centralizzata 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.
11. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett. a, b, c, d.

4.1.12. 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-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
3. 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. Gli strumenti tecnici di cui al punto 1 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. Gli strumenti tecnici di cui al punto 1 sono impiegati anche per i fini di cui alla categoria DE.AE

6. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione al punto 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati
5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.
6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.
7. Gli strumenti tecnici di cui ai punti 5 e 6 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. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 5 e 6;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

RESPOND (RS)

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

RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.
3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.
4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi.
5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di cybersecurity.
6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.
7. 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.

4.1.14. 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-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente
4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (*lessons learned*).
5. 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. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.
7. 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.
8. 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)

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

RC.IM-2: Le strategie di recupero sono aggiornate
1. Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.

4.1.16. 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-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione
1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT /CSIRT).

4.2.Affidabilità

4.2.1. Business Continuity e Disaster Recovery

A.BC-4: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti
1. Provider di infrastruttura: L'infrastruttura digitale deve essere dotata di soluzioni di DR e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA. Devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 8 ore e RPO 8 ore;
2. Public Cloud provider: devono essere presenti servizi di Disaster Recovery.

5.APPENDICE

Tabella 1-Indicatori minimi di servizio dell'Infrastruttura

Codice SLI	**Service level indicator (SLI)**	**Descrizione**	**Minimum Service Level Objective (SLO)**
SL1	Disponibilità	La percentuale di tempo in un anno in cui l'infrastruttura risulta essere accessibile e usabile	99,98% al netto dei fermi programmati (ovvero pari a 17h, 31m, 53s in un anno solare) 99,6 % comprendendo i fermi programmati (ovvero pari a 1 giorno 11h, 3m, 47s in un anno solare)
SL2	Attività di supporto - Support hours emergenze	L'orario in cui il servizio di supporto tecnico è operativo per emergenze.	24x7
SL3	Attività di supporto - Support hours (minime)	L'orario minimo in cui il servizio di supporto tecnico è operativo	Business hours: lunedì-venerdì, dalle 8 alle 18
SL4	Attività di supporto - First Support Response Time	Il tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta iniziale alla segnalazione da parte del soggetto	1h
SL5	Recovery Time Objective (RTO)	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery).	4h
SL6	Recovery Point Objective (RPO)	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery).	4h
SL7	Backup testing	Il numero minimo di test di restore (a partire dai dati di backup) eseguiti in un anno.	1
SL8	Comunicazione incidenti e data breach	L'intervallo di tempo massimo per notificare l'Amministrazione di un incidente o data breach, a valle della registrazione della segnalazione e classificazione dell'evento	1h dalla registrazione della segnalazione

Tabella 2 "caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio"

Best practices ANSI/TIA942, 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 danni 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.
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.

Allegato B2 - Caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità e portabilità dei servizi cloud per la Pubblica Amministrazione

Gennaio 2022, versione 1.0

1. PREMESSA

1. Il presente allegato definisce le caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità e portabilità dei servizi cloud per la Pubblica Amministrazione di cui all'art. 8, c. 3 del Regolamento, che possono ospitare, rispettivamente servizi e dati digitali della PA classificati, ai sensi del processo di cui all'art. 3 del Regolamento, quali ordinari, critici o strategici.
2. Le caratteristiche di sicurezza sono organizzate sulla base delle sottocategorie del Framework Nazionale per la Cybersecurity e la Data Protection (di seguito FNCS) e definite tenendo 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.
3. Sono, altresì, indicate raccomandazioni, la cui attuazione è demandata alle valutazioni di ciascun soggetto.
4. Ad eccezione dell'organizzazione di cybersecurity, il termine "organizzazione", che compare all'interno delle descrizioni delle categorie e sottocategorie, è da intendersi riferito almeno ai servizi cloud e al personale ad essi riconducibili a diverso titolo.

5. Ai fini del presente allegato, si intende per*:*

    a. **Regolamento**, 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, recante "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", adottato dall' AgID con Determinazione n. 628/2021 del 15 dicembre 2021;
    b. **Servizio cloud**, servizio cloud per la Pubblica Amministrazione di cui all'art. 1, co. 1, lett. p, del Regolamento;
    c. **Soggetto***,* il fornitore del servizio cloud;
    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 del servizio cloud;
    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 soggetto, da cui dipende il funzionamento del servizio cloud;
    f. **Catena di approvvigionamento *cyber***, la catena di approvvigionamento relativa a ciascun servizio cloud.
6. Fatto salvo dove diversamente specificato, i seguenti controlli si applicano ai servizi cloud di tipologia IaaS, PaaS e SaaS di cui all'art. 1, co. 1, lett. p, del Regolamento.

2. ORDINARI

2.1. Qualità

2.1.1. Qualità del servizio

QU.SE-1: Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore
1. 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. 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-2: Viene fornito un adeguato servizio di assistenza e supporto
1. È garantito il servizio di supporto e assistenza all'Amministrazione per il servizio cloud.
2. Il servizio di supporto e assistenza di cui al punto 1 è fornito almeno in lingua italiana tutti i giorni dell'anno a qualsiasi orario (24/7/365).
3. Il servizio di supporto e assistenza di cui al punto 1 è accessibile almeno tramite recapito telefonico e posta elettronica.
4. Il servizio di supporto e assistenza di cui al punto 1 prevede, inoltre, un sistema di risoluzione dei problemi (*troubleshooting*) a disposizione dell'Amministrazione, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i sistemi di gestione dei problemi (Case Management System).

QU.SE-3: Il soggetto dichiara la frequenza di aggiornamento del servizio
1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).

QU.SE-4: Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud
1. 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.

2.1.2. Pricing

QU.PR-1: Tracciamento, reportistica e trasparenza dei costi e della loro elaborazione
1. 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. Gli strumenti e le API di cui al punto 1 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-2: Notifica e monitoraggio dei costi
1. 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-3: Requisiti minimi per il capitolato dei prezzi
1. 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. Il soggetto fornisce all'Amministrazione:
   a. un documento contenente i termini e le condizioni, specificando in particolare qualora i prezzi siano forniti per un servizio al 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).

2.1.3. Livello del servizio (SLA)

QU.LS-1: 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. Il soggetto garantisce aderenza agli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) riportati in Tabella 1 "Indicatori della Qualità del Servizio" e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA). Il soggetto può comunicare all'Amministrazione eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali.
2. 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.
3. 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.

QU.LS-2: Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione
1. 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-3: Esistono contenuti e caratteristiche minimi per i Service Level Agreement
1. 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*);
   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. Terminazione del servizio;
   h. Requisiti di interoperabilità e portabilità;
   i. Riservatezza dei dati.

QU.LS-4: È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato.
1. 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.

2.2.Sicurezza

IDENTIFY (ID)

2.2.1. 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-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione
1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. 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-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione
1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto.
2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate.

3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione.

ID.AM-3: I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati
1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati e approvati da attori interni al soggetto.

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. È nominato, nell'ambito dell'articolazione di cui al punto 1, 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. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, 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. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.

2.2.2. 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-1: È identificata e resa nota una policy di cybersecurity
1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.
2. Il Documento di cui al punto 1 deve essere approvato dal soggetto e aggiornato almeno su base annuale o in corrispondenza di sostanziali variazioni all'interno dell'organizzazione.

ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity
1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity.
2. 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.

2.2.3. 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-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
1. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica 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. 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-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
1. 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. L'analisi del rischio tiene conto delle dipendenze interne ed esterne del servizio cloud.
3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.

2.2.4. 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-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
1. Sono definiti i processi di gestione del rischio inerente la catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

PROTECT (PR)

2.2.5. 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-1: 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. 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.
2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.
3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).
5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.

PR.AC-3: L'accesso remoto alle risorse è amministrato
1. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.
2. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.
3. 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. Esiste un log degli accessi eseguiti da remoto.

PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
1. 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. 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. 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-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.
2. 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-7: 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. 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. 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 informazioni trasparenti in merito alle funzionalità di autenticazione a più fattori accessibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione, con specifiche sui meccanismi adoperati per l'autenticazione (es. e-mail, sms o check biometrico).

2.2.6. 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-1: Il personale del soggetto è informato e addestrato
1. 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. L'addestramento e la formazione di cui al punto 1 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
   d. la definizione di ruoli e delle responsabilità
   e. politiche di accesso a sistemi, asset e risorse
   f. politiche di gestione delle informazioni e della sicurezza
   g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi
   h. requisiti per la non divulgazione/confidenzialità di informazioni

PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità
1. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.

2.2.7. 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-1: I dati memorizzati sono protetti
1.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.
2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud al trattamento dei dati e dei servizi dell'Amministrazione, fermo restando quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01, qualora sussistano motivate e documentate limitazioni di carattere tecnico, eventuali metadati necessari per l'erogazione del servizio cloud possono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate al di fuori del territorio dell'Unione europea. In tal caso, i citati metadati non possono contenere, anche in parte, i dati dell'Amministrazione.
3. 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.
4. Il soggetto garantisce autonomia all'Amministrazione nella gestione delle proprie chiavi crittografiche e, in particolare:
   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. È prevista la generazione di chiavi crittografiche segrete e private per uno scopo unico.

e. 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.
5. 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.
6. 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 d'accesso a repository

PR.DS-2: I dati sono protetti durante la trasmissione
1. 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-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
1. 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-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
1. 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. Sono adottate politiche di *Data Loss Prevention* coerentemente con la valutazione dei rischi.

PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
1. 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-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
1. 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.

2.2.8. 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-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
1. 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-3: Sono attivi processi di controllo della modifica delle configurazioni
1. 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. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.
3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. *rollback*) in caso di errori o problemi di sicurezza.

PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati
1. 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. Viene effettuato periodicamente un *backup* dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup
3. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette con crittografia forte 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 con crittografia forte.
4. Viene verificato periodicamente il ripristino (test di *restore*) delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
1. 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. 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. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
4. I piani di *business continuity* sono collaudati e comunicati alle parti interessate.
5. La documentazione di cui al punto 2 è resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.

PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità
1. Esiste un documento aggiornato di dettaglio che indica almeno:
a. le politiche di sicurezza adottate per gestire le vulnerabilità;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. 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]

2.2.9. 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-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
1. 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-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR.AC-3 e dei seguenti punti.
2. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di *cybersecurity* e limitati ai soli casi essenziali.
3. Sono adottati stringenti meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi.
4. Sono adottati meccanismi di gestione e controllo delle utenze privilegiate, in termini di limitazioni di natura temporale e delle funzionalità amministrative disponibili.
5. Tutti i log relativi alle sessioni di comunicazione remota e alle attività eseguite sui sistemi remoti, sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote.

2.2.10. 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-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. 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-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
1. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;
2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate.
3. Sono definite:
a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DETECT (DE)

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

DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
1. Ai fini di rilevare tempestivamente incidenti con impatto 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. 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. Sono definite:
a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a);
b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b);
c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c);
d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.
4. 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. 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. 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. 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. 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.

2.2.12. 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-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
1. Sono presenti sistemi di rilevamento delle intrusioni (*Intrusion Detection Systems* - IDS).
2. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.
3. È previsto un sistema di monitoraggio dei 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-4: Il codice malevolo viene rilevato
1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (*Endpoint Protection Systems* - EPS).
2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.

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

DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability
1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese note all'interno del soggetto.
2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. i ruoli, i processi e le responsabilità di cui al punto 2;
   b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.
4. 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)

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

RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
1. Il piano di risposta prevede l'esecuzione tempestiva della valutazione degli eventi rilevati tramite l'analisi e la correlazione di cui alla categoria DE nonché la disseminazione immediata degli esiti verso le articolazioni competenti del soggetto, anche ai fini della notifica all'Amministrazione e, su base volontaria, al CSIRT Italia, degli incidenti con impatto sul servizio cloud.

2.2.15. 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-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.
2. Sono eseguite periodicamente esercitazioni.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2;
   b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2;
   c. le modalità per le esercitazioni di cui al punto 3.

RS.CO-5: 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 awareness)
1. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e altre entità rilevanti e in linea con il contesto del soggetto.
2. 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.

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

RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)
1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei *penetration test* e *vulnerability assessment* di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto

2. 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. Esiste un documento aggiornato che descrive, almeno:
   a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2;
   b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.

RECOVER (RC)

2.2.17. 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-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento dei servizi cloud coinvolti da un incidente di *cybersecurity*.

2.3.Performance e scalabilità

2.3.1. Caratteristiche del servizio

PS.CA-1: Il servizio cloud presenta le caratteristiche tipiche ed è conforme agli standard di settore
1. 1. 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.

2.3.2. Scalabilità del servizio

PS.SC-1: Trasparenza sulle modalità e meccanismi di scalabilità
1. 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).

2.4.Interoperabilità e portabilità

2.4.1. Gestione remota

IP.GR-1: Sono disponibili API per la gestione remota del ciclo di vita del servizio

1. L'ambiente del servizio cloud 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. È disponibile una documentazione tecnica, fruibile dall'Amministrazione, in merito alle API esposte e gli endpoint SOAP e/o REST.

2.4.2. Interoperabilità

IP.IN-1: Sono disponibili API per funzionalità applicative
1. 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]

2.4.3. Portabilità

IP.PO-1: Sono disponibili funzionalità/API per import/export dei dati
1. 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-2: 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. 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. Sono implementati protocolli di rete cifrati e standardizzati per la gestione, l'importazione e l'esportazione dei dati. [PaaS, SaaS]
3. 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]

3. CRITICI

3.1. Sicurezza

IDENTIFY (ID)

3.1.1. 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-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
5. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).
6. 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. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 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. L'incaricato di cui al punto 2 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 82/2021.

3.1.2. 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-1: È identificata e resa nota una policy di cybersecurity
3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato
4. 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

3.1.3. 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-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
3. Le relazioni periodiche delle verifiche e dei test di cui al punto 1 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. Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.

ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
4. 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

3.1.4. 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-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione

3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa (*Shared Security Responsibility Model*-SSRM) all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale.
4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione.
5. È fornita una chiara definizione in merito alla condivisione delle responsabilità.

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

1. In merito all'affidamento di forniture 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-6, punto 2, nel processo di fornitura, già a partire dalla fase di progettazione;
   b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore;
   c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del 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:
      i. 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;
      ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.
2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1.

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

1. Le misure di sicurezza implementate 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-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

1. Esiste un documento aggiornato 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. 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. 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. Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.
5. È definito, documentato, approvato, comunicato, applicato e mantenuto un piano di *Remediation*.

PROTECT (PR)

3.1.5. 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-1: 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. 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, 2, 3, 4, 5, 6;
   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-3: L'accesso remoto alle risorse è amministrato

5. 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-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

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

3.1.6. 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-1: Il personale del soggetto è informato e addestrato

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

3.1.7. 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-1: I dati memorizzati sono protetti

7. Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui alla sezione 2.2.7, PR.DS-1, punto 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud, nonché al trattamento dei dati e dei servizi dell'Amministrazione, ivi inclusi i metadati, resta fermo, pertanto, quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01.
8. 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
9. 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.
10. Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 10 nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud.
11. Sono definite ed implementate procedure e misure tecniche misure 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.
12. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

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

2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti [SaaS]

3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto [SaaS]

3.1.8. 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 assets.

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
2. 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. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni
4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità
5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile.
6. È presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS]
7. È presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].

PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
1. 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-4: I backup delle informazioni sono eseguiti, amministrati e verificati
5. 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. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
6. 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. 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. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
9. Le strategie di *disaster recovery* sono collaudate e comunicate alle parti interessate.
10. 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. 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. Il documento di cui al punto 1 della misura PR.IP-12 dovrà essere aggiornato su base semestrale.

3.1.9. 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-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
2. Esiste un documento aggiornato di dettaglio recante i p3rocessi e le politiche di cui al punto 1.
3. Le attività di cui al punto 3 sono volte a verificare anche aspetti di sicurezza.
4. Gli aggiornamenti software sono consentiti solo da fonti pre-autorizzate.

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

3.1.10. 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-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
1-bis. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
b. sono adottate architettura ridondate di rete, di connettività, nonché applicative.
a. esiste un sito di *disaster recovery*.

DETECT (DE)

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

DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
9. 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

3.1.12. 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-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity
5. 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.
6. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 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.
7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5sono impiegati anche per i fini di cui alla categoria DE.AE
8. Esiste un documento aggiornato che descrive, almeno:
a. le politiche di sicurezza adottate in relazione ai punti 1, 3, 4 e 5;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati
1. Con riferimento alla sottocategoria PR.AC-3, viene rilevata la presenza di personale con potenziale accesso fisico o remoto non autorizzato alle risorse. A tal fine, sono presenti sistemi di sorveglianza e controllo di accesso, anche automatizzati.
2. Con riferimento alla sottocategoria ID.AM-1, vengono rilevati dispositivi (anche fisici) non approvati. A tal fine, fatti salvi documentati limiti tecnici, sono presenti almeno dei sistemi di controllo di accesso di rete.
3. Gli strumenti tecnici di cui ai punti 1e 2 sono aggiornati, mantenuti e ben configurati, nel rispetto delle politiche di cui alle categorie PR.AC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.
4. Esiste un documento aggiornato che descrive, almeno:
a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

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

RESPOND (RS)

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

RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
2. Le politiche e procedure per la gestione tempestiva degli incidenti di sicurezza sono riviste almeno su base annuale.
3. Il piano di risposta e le politiche e procedure di cui ai punti 1 e 2 includono dipartimenti interni critici, l'Amministrazione (se impattata) e tutte le terze parti interessate.
4. I piani di risposta agli incidenti sono collaudati e aggiornati ad intervalli pianificati o in caso di cambiamenti organizzativi o ambientali significativi
5. Sono definite e monitorate le metriche degli incidenti rilevanti in materia di *cybersecurity*.
6. Sono definiti e implementati processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza.
7. 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.

3.1.14. 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-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

4. Esiste un registro aggiornato delle esercitazioni effettuate e dei partecipanti, con le relative lezioni apprese (*lessons learned*).
5. 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. Sono definiti ed implementati processi, procedure e misure tecniche per le notifiche di violazione della sicurezza.
7. 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.
8. 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.

3.1.15. 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-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.
2. 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)

3.1.16. 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-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
3. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

3.1.17. 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-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione
1. Le attività di ripristino a seguito di un incidente sono comunicate alle parti interne ed esterne interessate (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT /CSIRT).

4. 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-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
6. Esiste un documento recante i processi di cui ai punti 1 e 2.

ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber
3. Si raccomanda, ove possibile e in relazione alla criticità di:
   a. valutare l'affidabilità tecnica di cui al punto 1, lettera d, anche tenendo conto:
      i. della disponibilità del fornitore a condividere il codice sorgente;
      ii. di certificazioni o evidenze utili alla valutazione della qualità del processo di sviluppo del software del produttore;
      iii. 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*;
      iv. 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:
      i. valutare la qualità e la sicurezza del codice sorgente, qualora reso disponibile dal produttore;
      ii. acquisire il codice oggetto dai beni e sistemi di information and *communication technology*;
      iii. confermare la corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito.

ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber.
2. 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-3: L'accesso remoto alle risorse è amministrato
6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione.
7. 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.
8. 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-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni

4. 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-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
3. Con riferimento ai censimenti di cui alla categoria ID.AM, esiste un documento aggiornato di dettaglio contenente almeno:
   a. le politiche di sicurezza adottate per la segmentazione/segregazione delle reti;
   b. la descrizione delle reti segregate/segmentate;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza;
   d. le modalità con cui porte di rete, protocolli e servizi in uso sono limitati e/o monitorati.

PR.AC-7: 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. 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-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità
3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2

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-1: I dati memorizzati sono protetti
13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio cloud. Il soggetto rende disponibile l'elenco all'Amministrazione.

PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

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 assets.

PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

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

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

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-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
7. Esiste un registro aggiornato delle manutenzioni e riparazioni eseguite.
8. 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. Il codice oggetto relativo agli aggiornamenti di cui al punto 3 viene custodito per almeno 24 mesi.

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-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.

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

PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.

DETECT (DE)

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

DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett. a, b, c, d.

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-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati
5. Con riferimento alla sottocategoria ID.AM-2, fatti salvi documentati limiti tecnici, sono presenti sistemi di controllo per il rilevamento dei software non approvati.
6. Con riferimento alla sottocategoria ID.AM-3, sono presenti sistemi di controllo per il rilevamento delle connessioni non autorizzate.
7. Gli strumenti tecnici di cui ai punti 5 e 6 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. Esiste un documento aggiornato che descrive, almeno:
   a. le politiche di sicurezza adottate in relazione ai punti 5 e 6;
   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-2: Le strategie di recupero sono aggiornate
1. Il piano di cui alla sottocategoria RC.RP-1 è mantenuto aggiornato tenendo anche conto delle lezioni apprese nel corso delle attività di ripristino occorse.

5. APPENDICE

Tabella 1 "Indicatori minimi della qualità del Servizio"

Codice SLI	Service level indicator (SLI)	Descrizione	Minimum Service Level Objective (SLO)
SL1	Disponibilità	La percentuale di tempo in un mese in cui il servizio cloud risulta essere accessibile e usabile. 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.	99.0%
SL2	Attività di supporto - Support hours emergenze	L'orario in cui il servizio di supporto tecnico è operativo per emergenze.	24x7
SL3	Attività di supporto - First Support Response Time	Il tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta iniziale alla segnalazione da parte del soggetto.	≤ 1h
SL4	Minor Release	L'intervallo di tempo massimo 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 retrocompatibili.	3 giorni
SL5	Major Release	L'intervallo di tempo massimo di preavviso previsto per dare comunicazione, accompagnata da release note, alla Amministrazione di Major Release. Per Minor Release si intendono modifiche al servizio che riguardano una sostanziale evoluzione delle funzionalità del servizio rispetto alla versione precedente.	1 mese
SL6	Backup	Numero minimo di test della procedura di restore eseguiti in un anno	1

Allegato C - Requisiti per la qualificazione dei servizi Cloud per la Pubblica Amministrazione

Gennaio 2022, versione 1.0

Sommario

1.Premessa

1. Il presente allegato descrive:
    a. l'elenco dei requisiti per la qualificazione dei servizi cloud per la Pubblica Amministrazione per i quattro livelli di qualificazione:
        i. qualificazione cloud di livello 1 (QC1), oggetto della sezione 2;
        ii. qualificazione cloud di livello 2 (QC2), oggetto della sezione 3;
        iii. qualificazione cloud di livello 3 (QC3), oggetto della sezione 4;
        iv. qualificazione cloud di livello 4 (QC4), oggetto della sezione 5.
    b. l'elenco dei requisiti per la qualificazione delle infrastrutture cloud tramite le quali sono erogati i servizi cloud per la pubblica amministrazione, per i quattro livelli di qualificazione:
        i. qualificazione infrastruttura di livello 1 (QI1), oggetto della sezione 6;
        ii. qualificazione infrastruttura di livello 2 (QI2), oggetto della sezione 7;
        iii. qualificazione infrastruttura di livello 3 (QI3), oggetto della sezione 8;
        iv. qualificazione infrastruttura di livello 4 (QI4), oggetto della sezione 9.

2. Ai fini del presente allegato, si intende per:
    a. **Regolamento,** 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, recante "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", adottato dall' AgID con Determinazione n. 628/2021 del 15 dicembre 2021;
    b. **Atto**, l'atto successivo adottato dall'ACN d'intesa con DTD ai sensi degli articoli 7, 8, 11 del Regolamento del quale il presente documento costituisce allegato;
    c. **Soggetto**, per i requisiti di cui alle sezioni 2,3,4,5 il fornitore di servizi erogati in modalità Cloud e a cui si rivolge il processo di qualificazione dei servizi cloud, per i requisiti di cui alle sezioni 6,7,8,9, il soggetto che detiene l'infrastruttura sottostante al servizio cloud oggetto di qualificazione;
    d. **Dati dell'Amministrazione,** i dati dell'Amministrazione di cui all'articolo 1, comma 1, lettera k) del Regolamento trattati mediante il servizio cloud erogato dal soggetto;
    e. **Metadati**, i dati, diversi dai dati dell'Amministrazione, necessari per il funzionamento e il monitoraggio del servizio cloud erogato dal soggetto, quali, ad esempio, la telemetria e gli indicatori tecnici (e.g., KPI e IP).

2. Requisiti per la qualificazione cloud di livello 1 (QC1)

2.1 Caratteristiche dei servizi cloud

Ai fini della qualificazione di livello QC1 è richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali **ordinari**, ai sensi dell'articolo 3 del Regolamento.

2.2 Certificazioni

Ai fini della qualificazione di livello QC1 sono richieste:

- una certificazione ISO 9001 – Sistemi di Gestione per la Qualità (SGQ) per il servizio cloud oggetto di qualifica;
- una certificazione ISO/IEC 27001:2013 – Sistema di gestione per la sicurezza delle Informazioni (SGSI) con estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019 per il servizio cloud oggetto di qualifica. In alternativa al suddetto requisito è possibile presentare certificazione *Cloud Security Alliance - Star Level 2*.

3. Requisiti per la qualificazione cloud di livello 2 (QC2)

Ai fini della qualificazione di livello QC2 è richiesto il rispetto dei requisiti per il livello di qualificazione QC1.

3.1 Caratteristiche dei servizi cloud

Ai fini della qualificazione di livello QC2 è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali **critici**, ai sensi dell'articolo 3 del Regolamento.

3.2 Certificazioni

Ai fini della qualificazione di livello 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 la qualificazione cloud di livello 3 (QC3)

Ai fini della qualificazione di livello QC3 è richiesto il rispetto dei requisiti per il livello di qualificazione QC2.

4.1 Caratteristiche dei servizi cloud

Ai fini della qualificazione di livello QC3 è richiesto, inoltre, il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità di cui all'Allegato B2 dell'Atto per i servizi cloud per la pubblica amministrazione che possono trattare dati e servizi classificati quali **strategici**, ai sensi dell'articolo 3 del Regolamento

4.2 Certificazioni

Ai fini della qualificazione di livello QC3 sono richieste:

- una certificazione ISO 22301- *Business Continuity* - Management System (Gestione della continuità operativa) per il servizio cloud oggetto di qualifica;
- una certificazione ISO/IEC 20000 (*Service Management*) per il servizio cloud oggetto di qualifica;
- una certificazione *Cloud Security Alliance - Star Level 2*.

5.Requisiti per la qualificazione cloud di livello 4 (QC4)

Ai fini della qualificazione di livello QC4 è richiesto il rispetto dei requisiti per il livello di qualificazione QC3 e dei requisiti definiti nella sezione 5.1.

5.1 Ulteriori requisiti

5.1.1 Requisiti in tema di controllo dei flussi

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

2. Tutti i flussi per l'erogazione del servizio cloud sono soggetti a procedure di approvazione, di monitoraggio e di controllo concordati con l'Amministrazione.

5.1.2 Requisiti in tema di cifratura e gestione chiavi e autonomia operativa

PR.DS-1: i dati memorizzati sono protetti

14. 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

15. E' garantito l'accesso esclusivo da parte dell'Amministrazione alle chiavi di cui al punto 1 e ai dati in chiaro dell'Amministrazione.

16. Il fornitore del servizio cloud mette a disposizione dell'Amministrazione un servizio di HSM in modalità dedicata.

17. Il soggetto 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 soggetto può avvalersi di competenze di terze parti, assicurandone, ove possibile, la fungibilità.

5.1.3 Requisiti in tema di verifica e controllo del personale

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

1. Il soggetto 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. Il soggetto 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 soggetto provvede nel senso tempestivamente.

6. Requisiti per la qualificazione infrastruttura di livello 1 (QI1)

6.1 Livelli minimi delle infrastrutture digitali

Ai fini della qualificazione di livello QI1 è richiesto il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali **ordinari**, ai sensi dell'articolo 3 del Regolamento.

6.2 Certificazioni

Ai fini della qualificazione di livello QI1 sono richieste:

- una certificazione ISO 9001 – Sistemi di Gestione per la Qualità (SGQ) per l'infrastruttura digitale oggetto di qualifica;
- un'autocertificazione che attesti la conformità allo standard ISO/IEC 27001:2013 – Sistema di gestione per la sicurezza delle Informazioni, per l'infrastruttura digitale oggetto di qualifica.

7. Requisiti per la qualificazione infrastruttura di livello 2 (QI2)

Ai fini della qualificazione di livello QI2 è richiesto il rispetto dei requisiti per il livello di qualificazione QI1.

7.1 Livelli minimi delle infrastrutture digitali

Ai fini della qualificazione di livello QI2 è richiesto, inoltre, il rispetto dei livelli minimi di cui all'Allegato A2 dell'Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali **critici**, ai sensi dell'articolo 3 del Regolamento.

7.2 Certificazioni

Ai fini della qualificazione di livello QI2 sono richieste:

- 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;
- la certificazione ISO/IEC 27001:2013 – Sistema di gestione per la sicurezza delle Informazioni per l’infrastruttura digitale oggetto di qualifica.

8. Requisiti per la qualificazione infrastruttura di livello 3 (QI3)

Ai fini della qualificazione di livello QI3 è richiesto il rispetto dei requisiti per il livello di qualificazione QI2.

8.1 Livelli minimi delle infrastrutture digitali

Ai fini della qualificazione di livello QI3 è richiesto, inoltre, il rispetto dei livelli minimi di cui all’Allegato A2 dell’Atto per le infrastrutture per la pubblica amministrazione che possono trattare dati e servizi classificati quali **strategici**, ai sensi dell’articolo 3 del Regolamento.

8.2 Certificazioni

Ai fini della qualificazione di livello QI3 sono richieste:

- una certificazione ISO 22301- Business Continuity-Management System (Gestione della continuità operativa) per l’infrastruttura digitale oggetto di qualifica.

9. Requisiti per la qualificazione infrastruttura di livello 4 (QI4)

Ai fini della qualificazione di livello QI4 è richiesto il rispetto dei requisiti per il livello di qualificazione QI3, e dei requisiti definiti nella sezione 9.1.

9.1 Ulteriori requisiti

9.1.2 Requisiti in tema di verifica e controllo del personale

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

1. 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. 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.