Polo Strategico Nazionale

Realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale ("PSN"), di cui al comma 1 dell'articolo 33-septies del d.l. n. 179 del 2012

CUP: J51B21005710007

CIG: 9066973ECE

Manuale tecnico sulle misure di sicurezza "MTMS"

Data: 24/04/2023

Ed. 1 - ver. 01

PSN-MTMS_v1.docx

QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
PIANO OPERATIVO			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	01	24/04/2023	Prima emissione

NUMERO TOTALE PAGINE:	118

AUTORE:	
Team di lavoro PSN	Unità operativa Risk & Compliance, Solution, Technology & Officer, Security & Information e con il supporto di tutte le funzioni interne coinvolte nel processo e Fornitori Soci

REVISIONE:	
Referente del Servizio	Paolo Trevisan

APPROVAZIONE:	
Direttore del Servizio	Antonio Garelli

LISTA DI DISTRIBUZIONE

INTERNA A:

- HR & Organization Officer
- Procurement Officer
- Communication Officer
- Legal Officer
- Financial Officer
- Marketing & Sales Office
- Solution Officer
- Risk & Compliance Officer
- Technology & Officer
- Security & Information Officer

ESTERNA A:

- Direttore dell'Esecuzione Contrattuale PSN
- Pubbliche Amministrazioni aderenti a PSN
- Soci gestori (TIM, Leonardo, Sogei)
- Subfornitori, subappaltatori (per quanto applicabile)

INDICE

1 EXECUTIVE SUMMARY

1.1 Scopo del documento

Il **Manuale tecnico sulle misure di sicurezza** (nel seguito "**MTMS**") **della società Polo Strategico Nazionale S.p.A.** ("**PSN**") descrive i trattamenti, le responsabilità e le misure di sicurezza adottate dal PSN per garantire la sicurezza del dato, in termini di Riservatezza, Integrità e Disponibilità.

Questo documento, per ogni servizio commercializzato in ambito descrive in ottemperanza al GDPR (REGOLAMENTO EU N. 679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI) l'elenco dei trattamenti con le relative responsabilità, le misure di sicurezza di cui all'art. 32 GDPR ovvero le misure tecniche organizzative indicate nelle Determinazioni ACN N. 306 e 307 /2022 in funzione della classificazione dei dati gestiti dalla PA, secondo la metrica di ACN (dato ordinario, critico e strategico).

L'esecuzione dei trattamenti, secondo l'art. 28 del GDPR, deve essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il Responsabile al Titolare (ed al rispetto delle istruzioni impartite). Nella fattispecie PSN S.p.A. utilizzerà l'Allegato E - Facsimile Nomina Responsabile del Trattamento dei dati personali della Convenzione stipulata fra PSN S.p.A. e DTD e il presente documento richiamato nell'Allegato E, per procedere alla nomina di un altro Responsabile del trattamento (di seguito "Sub-Responsabile del trattamento").

2 RIFERIMENTI

In questo capitolo si riporta un elenco delle principali fonti normative e dei documenti applicabili e di riferimento per il presente documento.

2.1 Normative di riferimento

[1] REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*Regolamento Generale sulla Protezione dei Dati o GDPR*);
[2] Provvedimento "Amministratori di sistema" del 27 novembre 2008 e successiva modifica del 25 giugno 2009
[3] PSNC **(Perimetro di Sicurezza Nazionale Cibernetica)** Decreto-legge 105/2019 (convertito con modificazione dalla Legge 18 novembre 2019, n. 133) - Adozione delle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, in conformità a quanto prescritto dal DPCM 81/2021
[4] Misure minime di sicurezza informatica per la PA (AgID GG.UU 4/2017)
[5] Framework Nazionale di Cyber Security e Data Protection 2.0
[6] Determinazione AgID n. 628/2021 e Determinazioni ACN 306/2022 e 307/2022 e relativi allegati

3 DEFINIZIONI E ACRONIMI

All'interno del documento si fa riferimento **alle definizioni** riportate nella tabella che segue.

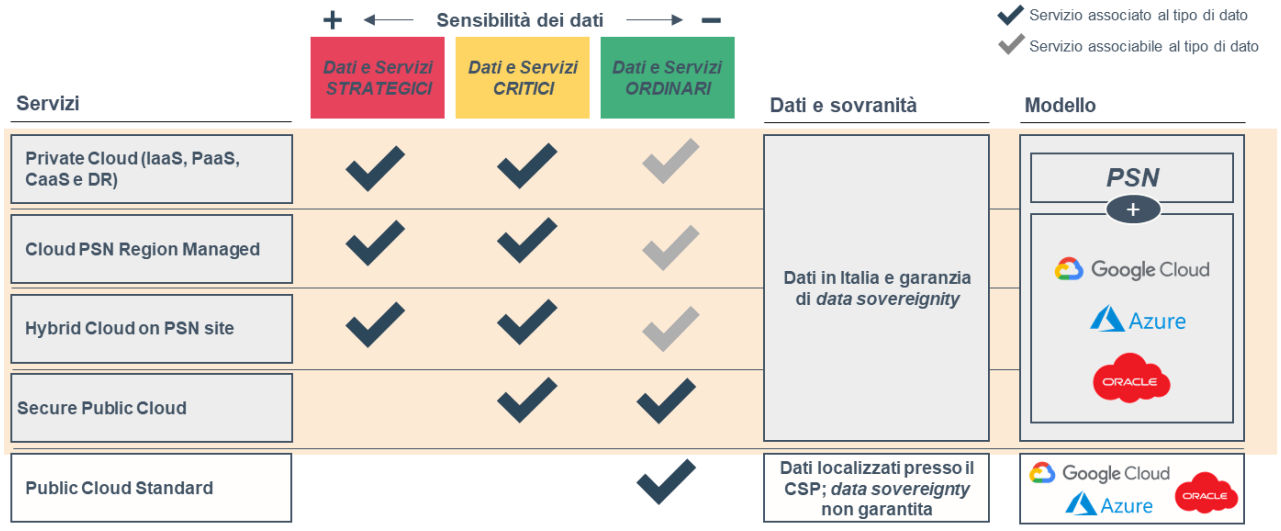
Glossario	Descrizione
PA	Pubbliche Amministrazioni
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
MTMS	Manuale tecnico sulle misure di sicurezza
Dati personali	Qualsiasi informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica e che possa fornire informazioni sulle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, etc
GDPR	*Il General Data Protection Regulation* è il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati
Normativa Privacy Applicabile	Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati ("GDPR") e le leggi nazionali tra cui il D. Lgs. 196/2003 e s.m.i (Codice della privacy), il D.lgs n. 101/2018 che specificano ulteriormente l'applicazione delle norme contenute nel GDPR, i provvedimenti del Garante Privacy, le Linee Guida *dell'European Data Protection Board* nonché gli orientamenti della giurisprudenza.
Responsabile ex art 28 GDPR	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che non opera sotto l'autorità o il diretto controllo del Titolare e, singolarmente o insieme ad altri, in virtù di apposito contratto di servizio o altro atto scritto equivalente, tratta i Dati Personali per conto del Titolare.
Titolare	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

4 AMBITO DI APPLICABILITA'

Il presente MTMS si applica a tutti i servizi previsti dal PSN e contrattualizzati dalla PA.

L'offerta del PSN è ampia e flessibile e permetterà alle PA di scegliere i servizi più idonei alle loro necessità, in base ai diversi modelli offerti. In particolare, il PSN offre soluzioni Cloud specifiche, sviluppate anche tramite specifici accordi industriali con CSP leader di mercato, tramite le quali è possibile offrire tutti servizi cloud richiesti, ma progettati specificamente per assicurare autonomia tecnologica, controllo diretto sul dato, cyber-resilienza, conformità ai requisiti di classificazione del dato (allineamento alle direttive ACN).

Tramite il PSN la PA potrà scegliere le soluzioni cloud più adatte a garantire innovazione ma anche privacy, sicurezza, compliance, efficienza e sovranità del dato come si evince dalla seguente figura:



Caratteristiche dei servizi cloud offerti alle PA

5 ANAGRAFICA FORNITORI DEL PSN

In questo capitolo sono elencati tutti i Fornitori che nei servizi di seguito dettagliati possono intervenire come responsabile esterno del trattamento:

TIM S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

Leonardo S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

Sogei S.p.A. ed eventuali sub responsabili (in caso di sub responsabili verrà fornita la lista relativa tramite il puntamento ad un apposito link o in modo esplicito al momento della contrattualizzazione con ciascuna Amministrazione).

6 DESCRIZIONE DEI MACRO-TRATTAMENTI

In questo capitolo sono descritti i macro-trattamenti riportati nei capitoli dei servizi, successivamente descritti:

Macro-Trattamenti	Descrizione	Possibili operazioni di trattamento dati personali associate alla categoria
Gestione delle infrastrutture e Service Management	Si intendono i servizi base di gestione delle infrastrutture necessarie all'erogazione del Servizio e i servizi di gestione al Cliente	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Trattamenti inerenti la Cybersecurity	Si intendono tutte le attività riferite alle attività di Security Operation tra cui anche la raccolta ed analisi dei log (es. FW, IDS, SIEM,..) ai fini dell'erogazione dei servizi di Cybersecurity (es. SOC);	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Supporto al Cliente per la migrazione e gestione.	Si intendono tutte le attività a corredo che il Cliente potrebbe chiedere come servizi professionali per gestire il suo contesto e per supportarlo durante il processo di migrazione di re-architect e di re-platform. Possono comportare attività di gestione sistemistica, middleware, applicativa. Compresi i servizi professionali di sicurezza.	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione
Erogazione al Cliente dei servizi di formazione	Si intendono tutte le attività a supporto del Cliente relativamente a Erogazione al Cliente dei servizi di formazione.	Raccolta, organizzazione, conservazione, estrazione, consultazione, cancellazione e distruzione

6.1 Macro-Trattamenti associati ai servizi dei Soci

Nella tabella a seguire viene descritta l'associazione tra i macro-trattamenti prima descritti ed i servizi erogati dai Soci:

Servizio Soci	TIM	LDO	SOGEI	Macro-Trattamenti
Spazi attrezzati	X	-	-	Gestione delle infrastrutture e Service Management
Connettività	X	-	-	Gestione delle infrastrutture e Service Management
COPS - servizi di gestione cliente (Help Desk di primo livello)	X	-	-	Gestione delle infrastrutture e Service Management
SERVICE MANAGEMENT - servizio di gestione del cliente	X	X	-	Gestione delle infrastrutture e Service Management
Business & Culture enablement	-	-	X	Erogazione al Cliente dei servizi di formazione
Sicurezza - Servizio CERT	-	X	-	Trattamenti inerenti la Cybersecurity
Security Operations	-	X	-	Trattamenti inerenti la Cybersecurity
Servizi professionali di sicurezza	X	X	-	Supporto al Cliente per la migrazione e gestione.
Paas Industry	-	X	-	Gestione delle infrastrutture e Service Management
Secure Public Cloud quota PSN	X	X	-	Gestione delle infrastrutture e Service Management
Public Cloud a PSN Managed	X	X	-	Gestione delle infrastrutture e Service Management
Hybrid Cloud on PSN site	-	X	-	Gestione delle infrastrutture e Service Management
IT Infrastructure - Controllo produzione	X	-	-	Gestione delle infrastrutture e Service Management
IT Infrastructure - Service Operations	X	X	X	Supporto al Cliente per la migrazione e gestione.
Servizio di migrazione	X	X	X	Supporto al Cliente per la migrazione e gestione.
Intra Migrazione	X	X	X	Supporto al Cliente per la migrazione e gestione.
Re-platform	X	X	X	Supporto al Cliente per la migrazione e gestione.
Re-architect	X	X	X	Supporto al Cliente per la migrazione e gestione.

7 SERVIZIO HOUSING

Il Servizio Infrastrutturale in modalità Housing Dedicato consiste nella messa a disposizione, da parte del PSN, di aree esclusive all'interno dei Data Center, dotate di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire elevati standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti.

7.1 Tipo dato - Trattamento e Responsabile del Trattamento

Per questo servizio è previsto il solo trattamento, da parte di PSN e TIM, di conservazione fisica dei dati personali nei Data Center dedicato al PSN.

8 SERVIZIO HOSTING

Il Servizio Industry Standard Hosting consiste nel rendere disponibile alle PPAA una infrastruttura fisica e dedicata.
Le modalità di erogazione sono:

- Hosting su rack condivisi: le PPAA avranno accesso a porzioni dedicate di rack condivisi con altre PPAA
- Hosting su rack dedicati: le PPAA avranno accesso a rack esclusivi/segregate

Il PSN è responsabile di tutti gli aspetti di gestione e manutenzione dell'infrastruttura hardware su cui è costruito il servizio.

8.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categorie Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

9 IAAS INDUSTRY STANDARD (Private, Shared, Storage)

Il Polo Strategico Nazionale ha una propria Cloud Platform con la quale erogare servizi IaaS ai clienti finali. La Cloud Platform è concepita nativamente in High Availability tra almeno 2 DC (HA-Zone) costituenti una specifica Region e in particolare 2 Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA Zone di ogni Region e le stesse Region sono interconnesse da un unico SDN Network layer in grado di consentire un modello di architettura flat che garantisca workload mobility e alta affidabilità intrinseca delle soluzioni Cloud.

L'infrastruttura, è ospitata all'interno di 4 Data Center, allestiti in doppia Region (2 DC + 2 DC) dotati di tutte le infrastrutture impiantistiche e tecnologiche necessarie a garantire i massimi standard qualitativi in termini di affidabilità, disponibilità e sicurezza fisica degli ambienti. TIM disponendo di questi diversi DC sul territorio nazionale atti all'erogazione di servizi IT, ne ha prescelti 4 in particolare per l'erogazione dei servizi Cloud PSN.

Questi DC sono:

- ***Region Nord***:
  - *Rozzano*
  - *Santo Stefano Ticino*

- ***Region Centro/Sud***:
  - *Acilia*
  - *Pomezia*

Il servizio IaaS Private garantisce delle risorse elaborative in uso esclusivo al cliente finale e tali risorse sono individuate attraverso Pool di Risorse che comprendono vCPU, vRAM e Storage Space e che in particolare indirizzano interi Bare Metal Hypervisors server come elementi minimi di configurazione. Quindi, è evidente che questo Cloud Service prevede risorse completamente dedicate e riservate ad un unico e solo cliente finale. Grazie alla disponibilità di questo Pool di Risorse, il cliente finale potrà autonomamente creare e gestire VMs e relativo vNetworking per consentire l'erogazione di un determinato modello di servizio applicativo installato all'interno delle VM sempre in modo del tutto autonomo. I Pool di Risorse possono essere allocati in modalità "Local Only" in una specifica HA Zone oppure in modalità "Stretched" e quindi con span in due HA Zone di una stessa Cloud Region.

Il PSN è responsabile della gestione completa dell'infrastruttura sottesa, e rende disponibile gli strumenti e le console per la gestione in autonomia degli ambienti virtuali contrattualizzati.

Il servizio IaaS Shared garantisce delle risorse elaborative al cliente finale e tali risorse sono individuate attraverso dei Pool di Risorse "elastiche" che comprendono vCPU, vRAM e Storage Space.
Le risorse sono definite elastiche perchè i Pool possono essere scelti in differenti sizing in funzione delle esigenze e, una volta allocati, possono essere pur sempre oggetto di resizing. Grazie alla disponibilità di questo Pool di Risorse, il cliente finale potrà autonomamente creare e gestire VMs e relativo vNetworking per consentire l'erogazione di un determinato modello di servizio applicativo installato all'interno delle VM sempre in modo del tutto autonomo.

Le risorse elaborative incluse nel Pool di Risorse sono ricavate su Bare Metal Hypervisors server condivisi con altri Pool di Risorse di altri clienti ma ad ogni modo ogni cliente avrà una netta separazione logica rispetto al contesto/workload di ogni altro cliente. I Pool di Risorse possono essere allocati in modalità "Local Only" in una specifica HA Zone oppure in modalità "Stretched" e quindi con span in due HA Zone. All'interno del proprio contesto, il cliente finale disporrà anche di un Catalogo di VM template da poter utilizzare per avviare appunto istanze di VM nelle proprie risorse elaborative disponibili. Il Catalogo conterrà VM template generati dal PSN come fornitore del servizio ma potrà anche avere una sezione privata e quindi gestita autonomamente dal cliente finale per la registrazione di VM template "proprietari" da poter mettere a disposizione dei propri utenti finali.

Il PSN è responsabile della gestione completa dell'infrastruttura sottesa, comprensiva degli strumenti di automation e orchestration.

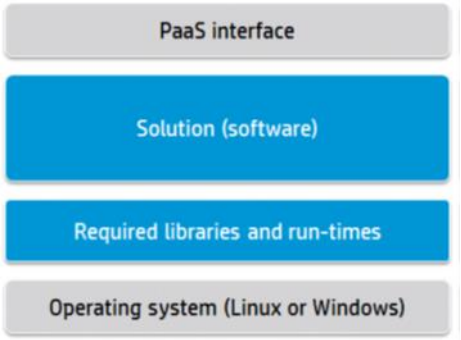
9.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10 SERVIZI PaaS

Il Servizio PaaS consiste nella messa a disposizione, da parte del PSN, di una piattaforma in grado di erogare elementi applicativi e middleware come servizio, come ad esempio i Data Base, astraendo dall'infrastruttura sottostante. Il PSN, in qualità di provider, si farà carico di gestire l'infrastruttura sottostante, comprensiva degli strumenti di automation e orchestration.

L'offerta dei servizi PaaS prevede un approccio strutturato in cui ogni componente della soluzione PaaS, come il sistema operativo, solution stack ed altri software necessari, è strettamente controllato in termini di utilizzo e configurazione e gestito dal PSN. In questo caso le soluzioni vengono "create" al momento della necessità. Una rappresentazione di questa strutturazione vede quattro livelli di componenti, evidenziati nell'immagine seguente



Componenti Servizio PaaS Industry

In particolare, questi componenti consisteranno in:

- Sistema operativo;
- Run-time e librerie necessarie;
- Soluzione caratterizzante – tipicamente un database, middleware, web server, ecc.;
- Un'interfaccia programmatica con cui controllare gli aspetti operazionali della soluzione.

Il PSN è responsabile dell'infrastruttura sottostante comprensiva degli strumenti di automation e orchestration e si compone dei sottoservizi nei seguenti paragrafi

10.1 PaaS DB

Il Database-as-a-Service è un servizio che consente agli utenti di configurare, gestire e ridimensionare database utilizzando un insieme comune di astrazioni secondo un modello unificato, senza dover conoscere o preoccuparsi delle esatte implementazioni per lo specifico database. Viene demandato al provider tutto quanto relativo all'esercizio e alla gestione dell'infrastruttura sottostante, comprese le operazioni di riconfigurazione della capacità elaborativa e delle repliche, mentre gli utenti possono così focalizzarsi sulle funzionalità applicative ed estrarre valore dai dati.

Tramite la console di gestione del servizio vengono messe a disposizione del cliente in particolare le funzionalità di:

- Creazione (o cancellazione) di un database;
- Modifica delle principali caratteristiche infrastrutturali dell'istanza DB e ridimensionamento ove non automatico;
- Configurazione di alcuni parametri del database;
- Attivazione di funzionalità aggiuntive, come ad esempio la replica dei dati su istanze passive (ove applicabile);
- Attivazione di funzionalità di backup od esportazione dei dati (ove applicabile).

Altre funzionalità avanzate di configurazione delle specifiche istanze database sono demandate alle relative interfacce di amministrazione native.

Il catalogo del servizio comprende:

- **Database relazionali** (**Oracle DB Enterprise e Standard, MySQL, PostgreSQL, Maria DB, …**) che supportano il modello dati relazionale e lo standard SQL di interrogazione. Sono quindi adatti a spostare carichi di lavoro di DB SQL preesistenti a casa del cliente su ambienti moderni e sicuri, in grado di garantire l'elevata affidabilità e le possibilità di crescita offerte dal Cloud;
- **Database NoSQL** (**MongoDB**, …) ottimizzati per trattare dati non strutturati, con volumi elevati o con caricamento di grandi quantità di informazioni in modelli dati flessibili e con bassa latenza.

10.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10.2 PaaS (Spid Enabling & Profiling)

In aggiunta ai servizi di Identity and Access Management che garantiscono i diritti di accesso alle componenti tecniche in ambito PSN (IaaS, PaaS, console unica di gestione, ecc.), viene reso disponibile dal PSN un servizio di Identity Management applicativo che consente di gestire in modo unificato e centralizzato l'autenticazione e l'autorizzazione per la messa in sicurezza delle applicazioni che migrano dentro il PSN.

Tale servizio ha lo scopo di integrare in modo facile e nativo le differenti esigenze di autenticazione e autorizzazione ad oggi previste all'interno del Codice dell'Amministrazione Digitale (CAD) ed in accordo con le normative vigenti in materia di trattamento dati riportate nel General Data Protection Regulation GDPR).

Il servizio mette a disposizione le seguenti funzionalità:

- Credenziali uniche di accesso alle applicazioni in perimetro e presidio efficace dei punti di accesso;
- Implementazione di policy di cambio password, autenticazione a due fattori o semplicemente auditing e monitoring dei log di accesso;
- Profilazione e segregazione delle informazioni in funzione dei propri privilegi: l'approccio di base si è concentra sulla creazione del "need-to-know". Le informazioni sensibili sono rese disponibili solo a quelle persone dotate di adeguate autorizzazioni e di un "need-to-know" di tali informazioni per l'esercizio delle loro funzioni;
- Controllo della diffusione delle informazioni: c'è una ragionevole probabilità che maggiori restrizioni sulla diffusione di informazioni sensibili riduce le possibilità di fughe di notizie e compromessi ("need-to-share").

I principali moduli funzionali disponibili all'interno del servizio fornito sono:

- **Identity Management & Governance**: è responsabile per la gestione del ciclo di vita delle identità digitali, gestisce la creazione, la modifica o la cancellazione delle identità, i loro attributi

e il rapporto tra identità e attributi all'interno del sistema IAM. Inoltre, è responsabile per la gestione del ciclo di vita dei ruoli e dei diritti di accesso per gestite le risorse di amministrazione;

- **Access Control & Management**: è responsabile di gestire l'assegnazione dei diritti di accesso alle identità e l'esecuzione, in caso contrario la convalida, dei diritti di accesso su sistemi finali;
- **Credential Management**: è responsabile per la gestione del ciclo di vita delle credenziali delle identità e la gestione dei relativi eventi, come la creazione, blocco, sblocco, etc.;
- **Multi Factor Authentication**: gestisce gli schemi di autenticazione utilizzati sul sistema IAM multifattore (gestione delle password, OTP Token, Smart Card, etc.). Per garantire la sicurezza dell'intera filiera applicativa il sistema di autenticazione multi-fattore deve garantire i livelli di sicurezza definiti all'interno della norma ISO/IEC DIS 29115
- **Logging & Reporting**: è il componente responsabile di raccogliere, correlare e normalizzare tutte le informazioni gestite dal sistema IAM per generare rapporti per uso amministrativo o di revisione contabile;
- **Federation Services**: rappresentano i servizi di federazione verso Identity Provider Esterni garantendo la piena compatibilità con i più diffusi sistemi di autenticazioni federati (SPID, eIDAS, CNS, etc.). In particolare, con l'introduzione dello SPID (Sistema Pubblico di Identità Digitale) promosso dall'Agenzia per l'Italia Digitale (AgID), il servizio proposto consente di accedere con un unico login ai diversi servizi on line di tutti i Soggetti Pubblici (PA) e Privati che adottano questo sistema di autenticazione. Il servizio SPID Enabling consente di connettere e abilitare i servizi web di aziende pubbliche e private al sistema di autenticazione SPID (Sistema Pubblico delle Identità Digitali) basandosi su un gateway di federazione SAML 2.0 nel quale sono state implementate le logiche e le specifiche tecniche SPID ed abilita ad un sistema di autenticazione federato verso tutti gli Identity Provider accreditati AgID.

10.2.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Gestione delle infrastrutture e Service Management	PSN, TIM, /Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10.3 PaaS Big Data

Il servizio consente la costruzione di Data Lake as a service, servizi di analisi dati batch, stream e real-time con scalabilità orizzontale e un servizio per la data governance:

- **Data Lake:** questa soluzione PaaS fornisce una piattaforma pronta all'uso che dispone di tutte le funzionalità necessarie a sviluppatori, Data Scientist e analisti per archiviare facilmente dati di tutte le dimensioni, forme e velocità. Tale soluzione permette l'archiviazione e analisi di file con scalabilità orizzontale, lo sviluppo di programmi con architettura altamente parallela, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes), essere progettato per essere utilizzato su infrastrutture cloud e supportare una vasta gamma di linguaggi (Python,R, Java, .Net, Scala).
- **Batch/Real time Processing:** questa soluzione PaaS fornisce una piattaforma pronta all'uso per sviluppare processi batch e in streaming basati su un motore di esecuzione in Memory e basato su scalabilità orizzontale e parallela. Tale soluzione consente l'analisi di grandi moli di dati sia in batch che in streaming, un paradigma di programmazione unico per l'analisi in batch e in streaming, lo sviluppo di programmi performanti con utilizzo di architetture scalabili orizzontalmente e parallele, mette a disposizione Tool per il Debug e l'ottimizzazione dei programmi sviluppati, è Integrabile con Schedulatori di Risorse Esterni (YARN, Kubernetes) e cloud ready, supporta una vasta gamma di linguaggi (Python,R, Java, .Net, Scala), espone api rest per il monitoraggio e il submit dei job da remoto, fornisce un pannello per il monitoraggio del job e dettagli per singolo job, integrabile con Storage Esterni (Data Lake Paas), fornisce funzionalità di autoscaling e fornisce meccanismi di caching su SSD.
- **Event Message: q**uesta soluzione PaaS rende disponibile una piattaforma pronta all'uso per sviluppare applicazioni e pipeline dati in real time inoltre deve fungere da Message Broker fornendo funzionalità di tipo Publish e Subscribe. Tale soluzione permette la gestione di grandi moli di eventi, lo sviluppo di programmi basati su architettura altamente parallela e scalabile orizzontalmente, fornire tool per il Debug e l'ottimizzazione dei programmi sviluppati, l'integrazione con Schedulatori di Risorse Esterni (YARN, Kubernetes) e progettato per essere utilizzato su infrastrutture cloud, supportare una vasta gamma di linguaggi (Python, R, Java, .Net, Scala), fornire funzionalità di autoscaling, implementare meccanismi di consegna degli eventi in ordine ed essere integrabile con framework di Stream Processing (Spark).
- **Data Governance:** questa soluzione PaaS fornisce una piattaforma pronta all'uso che mette a disposizione un unico punto di riferimento sicuro e centralizzato per il controllo dei dati. Sfruttando strumenti di "search and discovery" e i connettori per estrarre metadati da qualsiasi sorgente di dati, permette di semplificare la protezione dei dati, l'esecuzione delle analisi e la gestione delle pipeline, oltre ad accelerare i processi ETL. Tale soluzione consente di analizzare, profilare, organizzare, collegare e arricchire automaticamente tutti i metadati, implementare algoritmi per l'estrazione di Metadati e relazioni in modo automatico, supportare il rispetto delle normative e della privacy dei dati con il tracciamento intelligente della provenienza dei dati (data lineage) e il monitoraggio della conformità, semplificare la ricerca e l'accesso ai dati e verificare la validità prima di condividerli con altri utenti, produzione di dati relativi alla qualità del dato, definire in modo semplice e veloce i modelli e le regole necessarie per validare i dati e risolvere gli errori, permettere di supervisionare gli interventi per la risoluzione degli errori dei dati e mantenere la conformità rispetto a audit interni e normative esterne.

10.3.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

10.4 PaaS AI (Artificial Intelligence)

Il servizio mette a disposizione un set di algoritmi preaddestrati di Artificial Intelligence per utilizzarli in analisi del testo, audio/video o di anomalie ed una piattaforma per la realizzazione di modelli custom di machine/Deep Learning:

- **AI Platform:** questa soluzione PaaS rende disponibile una piattaforma pronta all'uso per costruire modelli di ML/DL facilitando l'accesso al dato mettendo a disposizione una ambiente collaborativo a cui partecipano sia esperti di contesto che Data Scientist. Tale soluzione permette il supporto di almeno le seguenti tipologie di sorgenti dati: NoSQl, SQL, Hadoop File Formats, Remote Data Sources, Cloud Object Storage, Cluster Hadoop, Rest Api; fornisce moduli configurabili per il data cleaning, wrangling e mining, strumenti e librerie per la visualizzazione dei dati, supporta le principali librerie per lo sviluppo di modelli di ML/DK (PyTorch, TensorFlow, ScikitLeran, H20,XGBoost, etc), supportare gli ultimi trend tecnologici (AutoML, Explanable AI), supportare una vasta gamma di linguaggi (Python, R) e strumenti a Notebook (Jupyter), permette la gestione della sicurezza di livello enterprise con la possibilità di implementare politiche RBAC, fornisce un approccio visuale di tipo Drag&Drop per lo sviluppo, la gestione intera del ciclo di vita di un progetto di datascience (Business Undestanding, Data Acquisition&Understanding, Modeling, Deployment), rende possibile interrogare i modelli attraverso degli endpoint Rest, monitorare le performance dei singoli modelli, supporta sia CPU che GPU, permette il Deploy dei modelli in versione dockerizzata e su Kubernetes, permette la creazione di pipeline di automation per la creazione di ambienti e il rilascio dei modelli, permette la creazione di Wiki per la condivisione delle informazioni relative ai singoli progetti, è integrabile con IAM esterni, permette il tracciamento e monitoraggio di tutte le azioni effettuate sulla piattaforma, permette la gestione centralizzata delle risorse di computing, permette la possibilità di creare policy custom per la protezione del dato e integrabile con sistemi di calcolo distribuiti (Spark, Hive, Impala, etc).
- **Semantic Knowledge Search:** questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di rendere facilmente accessibili le informazioni contenute all'interno del patrimonio informativo (documenti, immagini, video) utilizzando un motore di ricerca semantico in grado di interpretare richieste in linguaggio naturale. Tale soluzione permette di gestire contenuti in varie tipologie di formati (Documenti Word, pdf, pptx , email, immagini, video, etc), di indicizzare le informazioni contenute nei documenti, l'implementazione di un motore di ricerca di tipo full-text e di tipo semantico performante, l'esposizione di un'interfaccia in linguaggio naturale, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo), implementare meccanismo di auto apprendimento mediante feedback utenti, garantire la sicurezza del dato con vari tipologie di protezione (At rest, In Transit), garantire scalabilità orizzontale, esporre delle api per l'integrazione con sistemi esterni e essere integrabile con uno IAM esterno.
- **Text Analytics /NLP:** questa soluzione PaaS rende disponibile una piattaforma pronta all'uso in grado di estrarre informazioni da testo non strutturato.Tale soluzione consente di esporre delle api rest per l'inferenza dei modelli, l'estrazione di Entità dal testo (Persone, Luoghi, etc), estrazione di concetti chiave dal testo, estrazione del Sentiment, riconoscimento della Lingua, garantisce scalabilità orizzontale, supporto Load Balancing, il supporto almeno delle seguenti Lingue (Inglese, Italiano, Tedesco, Spagnolo), il tracciamento e il onitoraggio delle interrogazioni al sistema e la possibilità di essere eseguibile su Kubernetes o in versione dockerizzata.
- **Audio Analytics:** questa soluzione PaaS fornisce una piattaforma pronta all'uso in grado di applicare algoritmi basati su AI su fonti audio. Tale soluzione permette di analizzare grandi

volumi di audio, garantire scalabilità orizzontale, supportare Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni da fonti audio (Analisi rumore ambientale, Speaker Identification, Audio Insight), esporre un'interfacciata basata su api rest per l'inferenza, permettere la configurazione degli algoritmi da User Interface, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generazione di Eventi verso sistemi esterni, elaborazione sia in streaming che in batch, algoritmi estendibili attraverso componenti dockerizzate e deployable su Cluster Kubernetes.

- **Video Analytics:** questa piattaforma PaaS pronta all'uso è in grado di applicare algoritmi basati su AI su fonti video. Tale soluzione consente di analizzare grandi volumi di video, garantire scalabilità orizzontale, supporto al Load Balancing, mettere a disposizione algoritmi per l'estrazione di informazioni dai video (Detection, Classification, Identification, Counting, Density Estimation), esporre un'interfacciata attraverso api rest per la lettura dei metadati generati dagli algoritmi, fornire un portale web per la configurazione dei flussi video e degli algoritmi, fornire Report e Dashboard per il monitoraggio delle risorse del sistema e dei processi attivi, generare Eventi verso sistemi esterni, elaborazione dei video sia in streaming che in batch e fornire estendibilità degli algoritmi attraverso componenti dockerizzate.

10.4.1 Tipo dato - Trattamento e Responsabile del Trattamento

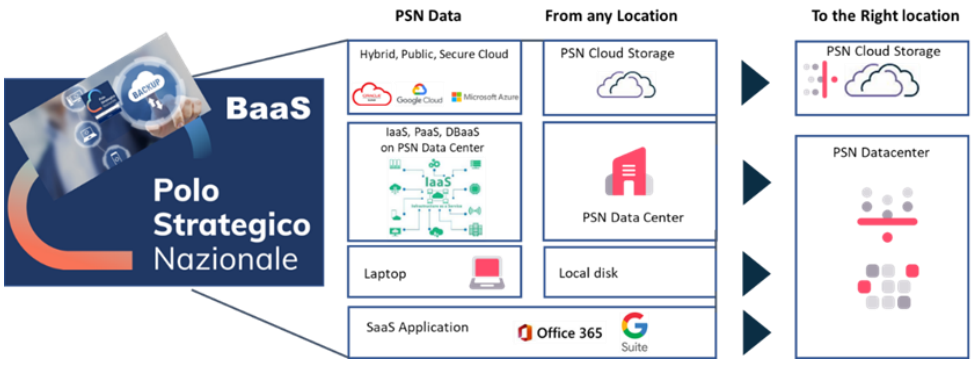
Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Leonardo ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

11 DATA PROTECTION (Opzione DR, BackUp, Golden Copy)

Quale ulteriore elemento di garanzia della protezione dei dati, oltre al backup standard, PSN mette a disposizione un **servizio opzionale** aggiuntivo che analizza i backup mensili allo scopo di intercettare eventuali contaminazioni malware silenti che comprometterebbero la validità di un eventuale restore in produzione. Tale funzionalità effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della golden copy; in particolare, quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul sistema sorgente e queste signature vengono utilizzate per convalidare i dati del backup. Una volta validate, tali signature vengono memorizzate con il backup stesso: ciò permette di eseguire automaticamente la verifica della consistenza dei dati salvati nel backup, utilizzando le signature salvate.

Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute, ecc) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

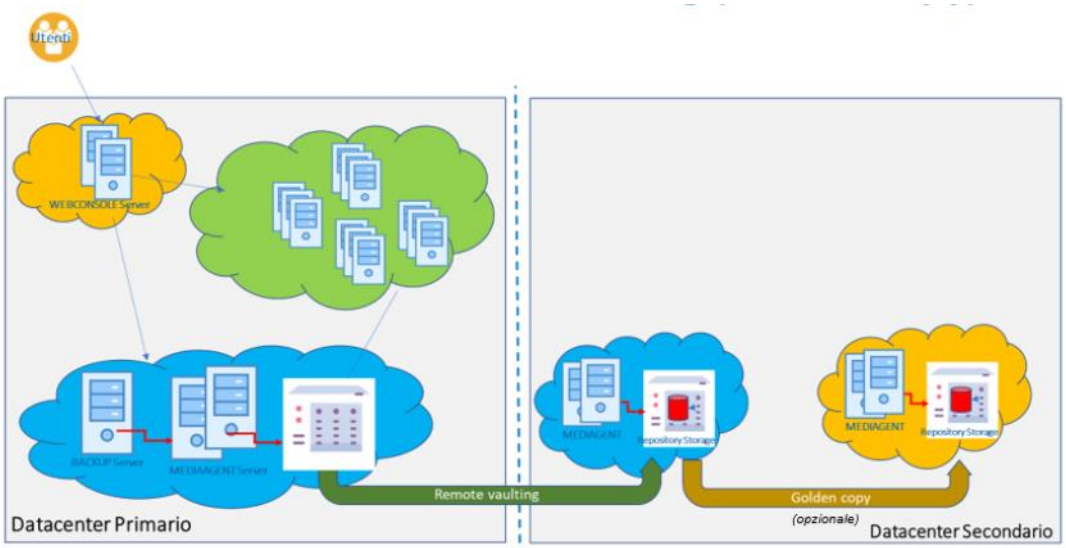
Tale servizio BaaS è erogato attraverso una console centralizzata attraverso la quale, in modalità self-managed, è possibile gestire la protezione dei vari contesti da proteggere (Files, VM, Container (k8), tutti i principali database come SAP-HANA, Exchange, SQL, Oracle, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, o i principali PaaS). Il servizio si basa su dei backup server che coordinano ed eseguono tutte le operazioni di backup e remote vaulting. Sulla base delle schedulazioni pianificate, il backup server esegue i jobs di backup.
Per tutti i backup sarà possibile effettuare una ulteriore copia secondaria al completamento della copia primaria.



Modalità di Erogazione Servizio BaaS: Golden Copy

L'utente dopo aver inserito le sue credenziali per accedere al portale BaaS potrà schedulare i job di backup sia su base giornaliera che su base settimanale attivare manualmente (on demand) la partenza del job di backup in funzione delle proprie esigenze.

Naturalmente, per ogni singolo sistema configurato sul servizio BaaS è possibile scegliere i dati (file, cartelle, VM, ecc.) che dovranno essere protetti, le modalità di backup (full o incrementale) e la retention da applicare.
Analogamente, per quanto riguarda il ripristino dei dati, l'utente, collegandosi al portale del servizio, può selezionare singoli file o interi set di backup (insieme di cartelle e file) tra quelli disponibili nel sistema scegliendo l'opportuna data di ripristino dei dati. Contestualmente, alla configurazione dei suoi backup, l'utente può scegliere di effettuare una copia secondaria dei dati di backup:



Esecuzione Copia di Back-up

Il Disaster Recovery "as-a-Service" (DRaaS) è invece il servizio di cloud computing che consente il ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso. Il modello as-a-service prevede che l'amministrazione stessa non debba essere proprietaria di tutte le risorse né occuparsi di tutta la gestione per il Disaster Recovery, affidandosi al service provider per un servizio completamente gestito. Il DRaaS si
basa sulla replica e sull'hosting dei server in un site del PSN diverso rispetto all'ubicazione primaria

11.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

12 CaaS

12.1 Servizio CaaS

ll Servizio Infrastrutturale in modalità CaaS consiste nella messa a disposizione, da parte del PSN, di una infrastruttura in grado di distribuire e gestire tutte le applicazioni basate su container in carico all'Amministrazione all'atto della stipula del Contratto, nonché di eventuali variazioni in corso d'opera.

Il servizio offerto si basa sul progetto **Open Source OKD,** già noto come OpenShift Origin (distribuzione community di openshift), una soluzione che nasce dall'evoluzione di Kubernetes, noto progetto open source per l'orchestrazione dei container, oggi mantenuto dalla Cloud Native Computing Foundation (CNCF), a cui sono aggiunte funzionalità di sicurezza e ottimizzazioni per il deploy in ambiente multi-tenant, progettate specificamente per ambienti di livello "enterprise". Il "motore" Kubernetes rimane dunque un componente "core" del progetto di community (container cluster management): il vantaggio dell'approccio Open Source è il contributo attivo di una community di partner in continua espansione che, attraverso la proposizione di soluzioni integrative (storage, networking, ISV, integrazioni IDE e CI compatibili con OpenShift Container Platform), rendono il prodotto più versatile ed innovativo. Essendo un servizio basato sull'astrazione dei container, può essere utilizzato su qualsiasi ambiente, per i vari ambiti di servizio previsti nell'offerta. Tutte le funzionalità aggiuntive della piattaforma accelerano la produttività degli sviluppatori, assicurando alle applicazioni la portabilità nel cloud ibrido, grazie al supporto di una community estesa.

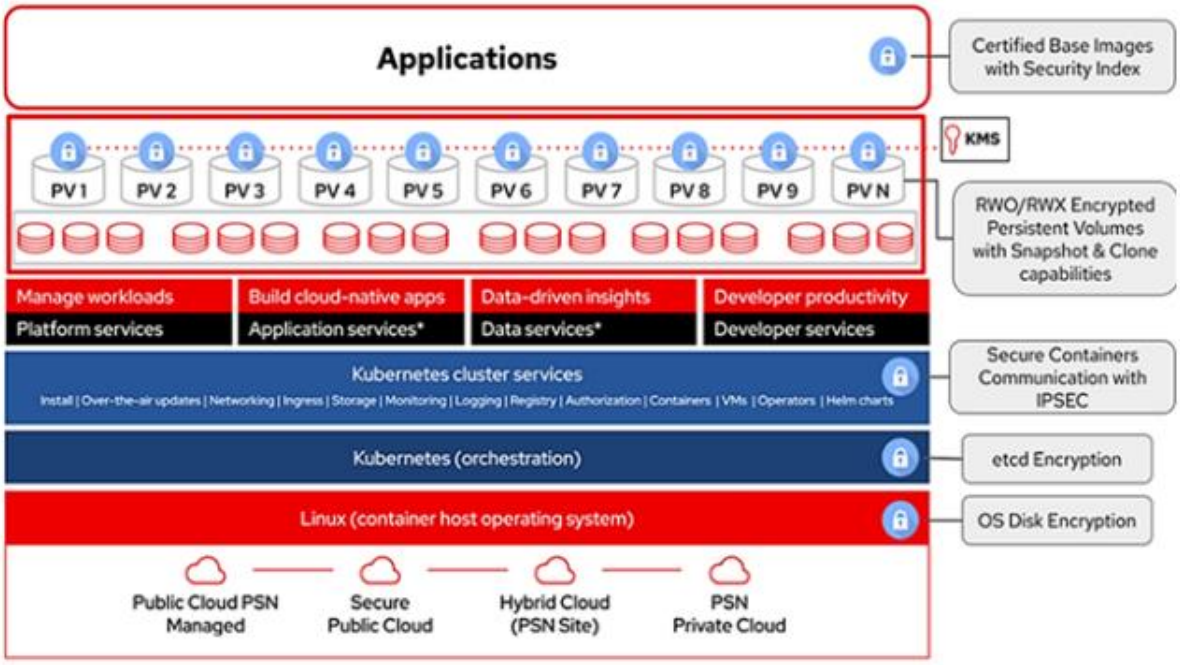
In particolare, per l'erogazione del servizio sarà utilizzata la distribuzione Red Hat di OpenShift, di cui OKD è il corrispondente progetto parallelo di community, su cui è basata appunto questa distribuzione: come per tutte le distribuzioni Red Hat, sul portale di accesso (access.redhat.com) è sempre disponibile il relativo codice sorgente, per ogni componente software RPM: il codice è quindi aperto. La distribuzione Red Hat di OpenShift aggiunge alla corrispondente distribuzione gemella di community, su cui si basa, il necessario livello di affidabilità che deriva dalla costante revisione di un team di esperti dedicati, oltre ad ulteriori funzionalità per la produttività e la sicurezza, tra cui registro, reti, telemetria, sicurezza, automazione, anch'essi basati a loro volta su altri progetti open source, che aiutano a sfruttare meglio il potenziale del software di orchestrazione, tra cui:

- Registro - es. Atomic Registry, Docker Registry.
- Rete – es. OpenvSwitch;
- Telemetria - es. Heapster, Kibana, Hawkular, Elastic.
- Sicurezza – es. LDAP, SELinux, RBAC, OAUTH.
- Automazione – es. Ansible

In seguito al deployment di cluster e applicazioni, la gestione del ciclo di vita di queste componenti, le console destinate a operatori e sviluppatori e la sicurezza diventano aspetti di fondamentale importanza. Red Hat OpenShift offre installazione, aggiornamenti e gestione del ciclo di vita automatizzati per tutte le componenti dello stack del container: sistema operativo, Kubernetes, servizi e applicazioni del cluster. Ne risulta una piattaforma applicativa Kubernetes più sicura e sempre aggiornata, priva delle complessità tipiche degli aggiornamenti manuali e seriali, e senza interruzioni

dell'operatività. La piattaforma si integra con Jenkins e altri strumenti standard di integrazione e deployment continui (CI/CD), nonché con gli strumenti e i flussi di lavoro integrati di OpenShift, per creare applicazioni sicure; integra container OCI/Docker e Kubernetes certificati da Cloud Native Computing Foundation (CNCF) per l'orchestrazione dei container, ed altre tecnologie open source. Le immagini dei container realizzate con lo standard **Open Container Initiative (OCI)** assicurano la portabilità tra le workstation di sviluppo e gli ambienti di produzione di OpenShift Container Platform.

La piattaforma può essere quindi utilizzata nei diversi ambiti previsti in modo uniforme, fornendo sia al gestore che all'utilizzatore un'esperienza coerente, omogenea e replicabile. Questa caratteristica consente una fruizione nei diversi ambiti di servizi proposti dal bando, secondo lo stesso schema di gestione: l'architettura proposta è quindi identica al variare dell'ambito di applicazione; questo è reso possibile dalla portabilità di OpenShift e dagli strumenti automatici di installazione e interfacciamento che astraggono dalle complessità e le specificità implementative.



Architettura OCI

12.1.1 Tipo dato - Trattamento e Responsabile del Trattamento

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

13 SERVIZI CSP

13.1 Public Cloud PSN Managed

Il Public Cloud PSN Managed realizza un modello di servizio del tutto analogo al Public Cloud del CSP (o Hyperscaler), ma rispetto ad esso permette di implementare una logica di separazione logica e fisica, sia nella gestione operativa che nel rilascio e controllo del software di base che caratterizza il servizio. La Region dedicata permette al personale del PSN di esercitare direttamente il controllo sui servizi del CSP, a tutti i livelli di esecuzione, per l'erogazione dei servizi dedicati alle PA:

- Hardware.
- Software (gestione e rilascio in modalità quarantena).
- Rete.
- Accesso e identità nella gestione Il PSN disporrà di istanze del cloud Hyperscaler aggiungendo i propri domini, indirizzi IP, branding, fatturazione e sarà integrato con servizi di Crittografia del PSN stesso.

Queste istanze possono essere totalmente disconnesse nel caso sorga la necessità' di tutelare la sicurezza nazionale. Tale Region dedicata può essere usata per i massimi livelli di confidenzialità dei dati grazie alla sua implementazione dedicata al PSN, garantendo però allo stesso tempo tutti i vantaggi di un cloud Hyperscaler quali ad esempio elasticità', completezza di servizi, innovazione e scalabilità.

Tale servizio permetterà alle Amministrazione di accedere a servizi dei CSP erogati da «Region» dedicata al PSN, con separazione logico/fisica e gestione operata da personale PSN. Le caratteristiche salienti del Public Cloud PSN Managed sono:

- Residenza dei dati in Italia.
- Controllo operativo affidato al Managed Service Provider (MSP), nel caso specifico TIM.
- Localizzazione nei Data Center del CSP, ma con segregazione fisica degli apparati dalle Region Pubbliche-
- Control Plane locale e disconnesso dal CSP-
- BYOID, ovvero liberta' di scegliere un sistema di identity proprietario.
- Ampia compatibilita' e offerta di servizi basati su Open-Source Software (OSS).
- Nessun accesso diretto del CSP all'infrastruttura o al software.
- Connettivita' verso l'esterno integralmente gestita da personale TIM o PSN
- Utilizzo dei servizi di sicurezza forniti da Google, ma gestiti da TIM.
- Ampio supporto dei servizi CSP tra cui AI/ML, Data Analytics, servizi di containerizzazione e servizi forniti da terze parti
- Gestione mediante strumenti e servizi basati su uno stack OSS, con API aperte e strumenti che assicurano semplicità, coerenza e portabilità in linea con i principi di Cloud Switching della recente proposta dell'EU Data Act.
- Gestione di tutta la Supply chain, dal rilascio del software, alla gestione dell'hardware

13.1.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Google)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Google ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

13.1.2 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Oracle)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, TIM, Oracle ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo

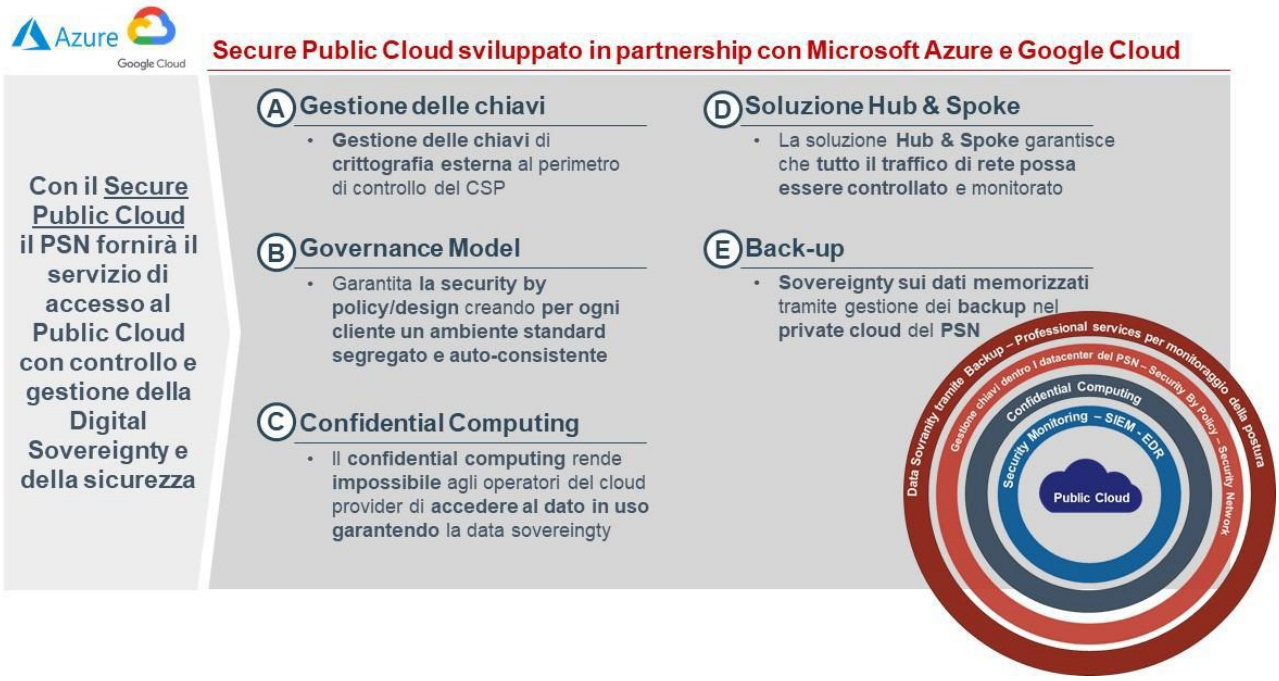
13.2 Secure Public Cloud

Il Secure Public Cloud è un servizio che si basa su Region pubbliche degli Hyperscaler (Microsoft Azure e Google Cloud GCP) a cui vengono aggiunti tutti gli elementi di sicurezza descritti nella documentazione tecnica (Chiavi esterne, backup, template, servizi professionali).

L'architettura del servizio "Secure Public Cloud" è basata su due componenti principali:

- **Public Cloud:** La componente **Hyperscale Public Cloud,** erogata da una *Region* collocata sul territorio nazionale, ai cui servizi vengono applicate configurazioni, policy e controlli di sicurezza, al fine di garantire ai clienti ambienti di elaborazione segregati aventi una sicurezza di base adeguata agli scopi del PSN;
- **Security & Governance:** Una componente, erogata dal Data Center del PSN distribuiti sul territorio Nazionale, nella quale verranno configurati servizi atti a garantire l'adeguato livello di sicurezza dei servizi erogati sul Public Cloud (Gestione Chiavi e Backup).

Di seguito, sono indicati i servizi di base erogati dal SPC per le pubbliche amministrazioni aderenti:



Servizi Erogati dal Secure Public Cloud

13.2.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Google)

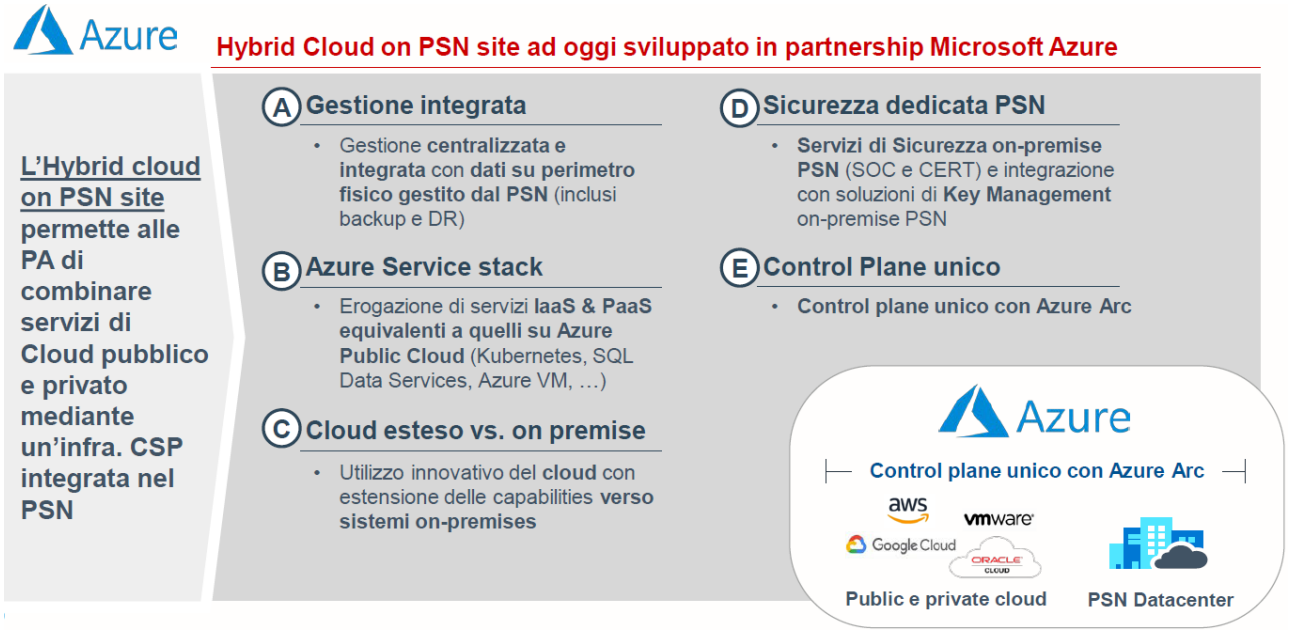
Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Google ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Google ed eventuali Subresponsabili

13.2.2 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Microsoft)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Microsoft ed eventuali Subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Microsoft ed eventuali Subresponsabili

13.3 Hybrid Cloud on PSN Site

L'Hybrid Cloud on PSN site permetterà alle PA di combinare i servizi privati e ibridi dei CSP (Microsoft Azure), su infrastruttura sicura PSN.



Servizi Erogati dall'Hybrid Cloud on PSN

Il servizio mette a disposizione infrastrutture iperconvergenti dedicate:

- Basate su **soluzioni HCI** (Hyperconverged Infrastructure) **dedicate** a ciascun cliente e **ubicate all'interno** dei Data Center del **PSN**;
- Registrate nelle **subscription dei clienti,** che diventeranno «deployment target» utilizzabili attraverso il **control plane di Azure** (Portale, Powershell, CLI, Rest API, …) per mezzo del servizio Azure Arc.;
- Caratterizzate da un **Management Plane** formato da**:**
  - Una componente rimanente sull'**area On-premise** del servizio (Admin Center);
  - Una componente che sfrutta i **servizi cloud Azure** per le funzionalità di monitoraggio, gestione aggiornamenti, raccolta eventi di sicurezza e controllo security posture.

13.3.1 Tipo dato - Trattamento e Responsabile del Trattamento (CSP Microsoft)

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)	Gestione delle infrastrutture e Service Management	PSN, Leonardo, TIM, Microsoft ed eventuali subresponsabili
	Trattamenti inerenti la Cybersecurity	PSN, Leonardo, Microsoft ed eventuali Subresponsabili

14 SERVIZI DI MIGRAZIONE, EVOLUZIONE E PROFESSIONAL SERVICES

Il PSN renderà disponibili risorse professionali in grado di poter supportare le Amministrazioni in tutte le attività che si renderanno necessarie nelle diverse fasi del progetto, a partire dalla definizione della metodologia di migrazione (re-host, re-architect, replatform), proseguendo nella fase di riavvio degli applicativi, nei regression test e terminando nel supporto all'esercizio.

14.1 Tipo dato - Trattamento e Responsabile del Trattamento

Potrebbero essere svolti trattamenti di Dati Personali e Personali Particolari, nell'erogazione dei servizi professionali.

Tipologia Dati e Categoria Dati	**Macro-Trattamenti**	**Responsabili dei Trattamenti**
Riportati nella lettera di nomina (Allegato E)		
	Supporto al Cliente per i servizi di migrazione, di re-architect e di re-platform e di gestione	PSN, TIM, Leonardo, Sogei e loro eventuali Sub-Responsabili

15 BUSINESS & CULTURE ENABLEMENT

La trasformazione digitale deve essere accompagnata non solo da un'innovazione tecnologica, ma soprattutto da un cambiamento delle metodologie di lavoro e dall'organizzazione dello stesso. Cambiare la cultura delle amministrazioni aderenti vuol dire agire sulla leadership e sulla collaborazione tra le persone.
Disegnare e produrre servizi e prodotti digitali per il bacino di utenza delle Amministrazioni aderenti, significa anche adottare modelli di lavoro omogenei; l'attenzione alla user experience consente infatti di rendere questa cultura una prassi da applicare sia all'interno dell'Amministrazione che verso gli utenti finali.
Punti nodali di questa trasformazione sono il change management ed il modello formativo. Per questi motivi, il PSN prevede di mettere a disposizione delle amministrazioni entrambi questi servizi.
Per quanto riguarda il Change Management si prevede un servizio di consulenza organizzativa che progetterà con le Amministrazioni i passi per eseguire il processo di digital trasformation relativamente a:

- Modello organizzativo;
- Competenze e modello manageriale;
- Tool Collaborativi;
- Employee experience;
- Modello di innovazione.

Inoltre, sarà disponibile un servizio che consente di erogare formazione tramite l'uso delle tecnologie multimediali e offrire la possibilità di erogare digitalmente i contenuti attraverso Internet o reti Intranet. Per l'utente rappresenta una soluzione di apprendimento flessibile, in quanto personalizzabile e facilmente accessibile.
Il servizio prevede l'erogazione, su una piattaforma messa a disposizione dal PSN, di corsi base a catalogo differenziati in base alle esigenze formative e corsi personalizzati secondo le esigenze dell'Amministrazione. In aggiunta ai due servizi precedentemente indicati se ne definisce uno di supporto specialistico per gli ulteriori aspetti metodologici e didattici, che prevede:

- affiancamento all'utente volto ad istruirlo all'uso delle funzioni del sistema di e-learning;
- gestione della comunicazione con gli utenti tramite i sistemi di messaggistica della piattaforma;
- ulteriore formazione trasversale con corsi specifici definiti a catalogo e/o customizzati su esigenze dell'Amministrazione.

In base alle necessità delle singole amministrazioni aderenti sarà individuato il mix di figure professionali necessarie, tra quelle messe a disposizione dal PSN, che effettuerà le attività richieste.

15.1 Tipo dato - Trattamento e Responsabile del Trattamento

Sono previsti trattamenti di raccolta e conservazione di Dati Personali Comuni per i quali verranno garantite le istruzioni presenti nella lettera di nomina (Allegato E).

Tipologia Dati e Categoria Dati	Macro-Trattamenti	Responsabili dei Trattamenti
Riportati nella lettera di nomina (Allegato E)		
	Erogazione al Cliente dei servizi di formazione	PSN, Sogei ed eventuali Subresponsabili

16 ALLEGATO - Misure di sicurezza e compliance

In questo capitolo sono elencate le misure definite by design e by default che, come da Art.32 del GDPR, garantiscono un livello di sicurezza adeguato al rischio dei servizi in ambito.

16.1 Misure derivanti dal provvedimento del Garante Privacy del 27/11/2008 in tema "Amministratori di Sistema"

Requisito
L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell´esperienza, della capacità e dell´affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un´attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

16.2 Determinazioni AgID e ACN – Misure di sicurezza per qualificazione infrastrutture/servizi per la PA

Le misure di sicurezza per la qualificazione delle Infrastrutture e dei servizi per la PA secondo la determinazione AgID (**Determinazione n. 628/2021)** e ACN (**Determinazioni 306/2022 e 307/2022** e relativi allegati), sono soddisfatte dalle certificazioni come da tabella:

QUALIFICA AGID - Circolari AGID n.2 e n.3 del 2018

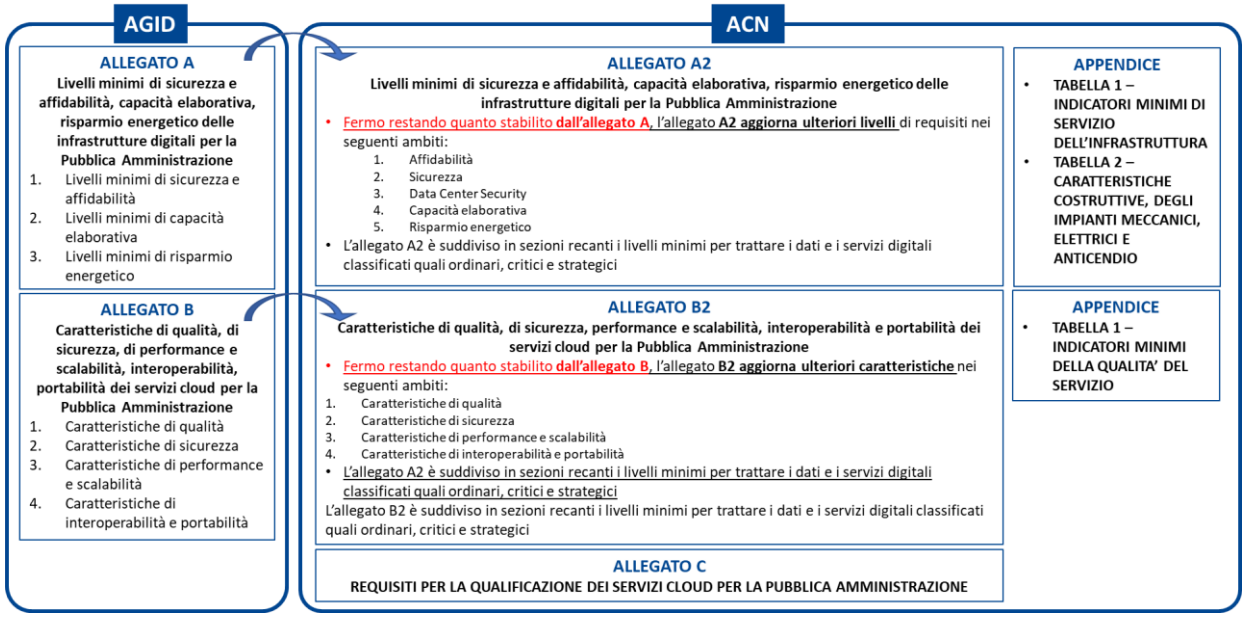
- Definizione **tipologia di qualifica:** qualifica di «**tipo C**» → **CSP /** qualifica di «**tipo A**» → **servizi IaaS/PaaS /** qualifica di «**tipo B**» → **servizi SaaS**

REQUISITI PER LA QUALIFICAZIONE SERVIZI CLOUD PER LA PA – DIC. 2021/GEN. 2022

Criteri definiti da AGID e Agenzia Nazionale per la Cybersicurezza (ACN), d'intesa con il Dipartimento per la Trasformazione Digitale (DTD)*

Tipologia dati	Requisiti per qualificazione servizi cloud PA		Requisiti per qualificazione infrastruttura	
	Qualificazione prevista	Certificazioni richieste	Qualificazione prevista	Certificazioni richieste
Ordinari	Livello 1 **(QC1)**	È richiesto il conseguimento delle seguenti certificazioni: **– ISO 9001** **– ISO 27001** **– ISO 27017** e **27018** (o in alternativa **CSA STAR LEVEL 2**)	Livello 1 **(QI1)**	- Conseguimento della certificazione **ISO 9001** - Autocertificazione che attesti conformità a standard **ISO 27001**
Critici	Livello 2 **(QC2)**	In aggiunta a quanto già previsto per **QC1**, è richiesta: - Autocertificazione che attesti conformità a standard **ISO 22301 e ISO 20000**	Livello 2 **(QI2)**	In aggiunta a quanto già previsto per **QI1**, è richiesta: - Autocertificazione che attesti conformità a standard **ISO 22301** - Conseguimento della certificazione **ISO 27001**
Strategici	Livello 3 **(QC3)**	In aggiunta a quanto già previsto per **QC2**, è richiesto il conseguimento delle seguenti certificazioni: **– ISO 22301** **– ISO 20000-1** **– CSA - STAR Level 2**	Livello 3 **(QI3)**	In aggiunta a quanto già previsto per **QI2**, è richiesto il conseguimento delle seguenti certificazioni: **- ISO 22301**
	Livello 4 **(QC4)**	In aggiunta a quanto già previsto per **QC3**, non sono richieste ulteriori certificazioni, ma solo il rispetto di requisiti specifici.	Livello 4 **(QI4)**	In aggiunta a quanto già previsto per **QI3**, non sono richieste ulteriori certificazioni, ma solo il rispetto di requisiti specifici.

Nei seguenti paragrafi sono riportate le misure di sicurezza di dettaglio organizzate come da figura allegata:



16.2.1 Requisiti AgID Allegato A

ID Requisito	Specifica Requisito
IN-CE-01	L'Amministrazione che eroga servizi ad altre amministrazioni deve formalizzare e pubblicare le informazioni relative ai servizi tramite il CED ricorrendo ad un apposito catalogo servizi, in conformità alle best practice ITIL. Il catalogo deve essere gestito e manutenuto attraverso un processo aderente alle best practice sul service catalogue management ITIL o alle linee guida riportate dallo standard ISO/IEC 20000-2.
IN-CE-02	L'Amministrazione che eroga servizi ad altre amministrazioni deve rendere nota la capacità di elaborazione totale del CED, quella occupata, quella libera per soddisfare i propri piani di capacity e quella a disposizione di Amministrazioni ospitate. Nello specifico, per ciascuna misura, l'Amministrazione deve dichiarare: - la superficie della sala CED o l'equivalente in numero di rack o di unità rack (U); - il numero e la tipologia di server fisici o di server farm disponibili, fornendo la capacità computazionale totale ottenuta come somma di memoria RAM disponibile [in GB], somma di CPU/Core e vCore, MIPs per gli apparati Mainframe, storage [in TB].
IN-RE-01	L'Amministrazione deve determinare con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura del DC e quella sostenuta per gli apparati.
IN-RE-02	L'Amministrazione deve avere adottato formalmente procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)
IN-SA-DC-08-01	L'Amministrazione deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.
IN-CE-03	La capacità elaborativa del CED deve essere gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000- 2.
IN-SA-DC-01-01	L'Amministrazione garantisce il presidio operativo del Data Center 24/7/365.
IN-SA-DC-02-01	L'Amministrazione deve dimostrare che gli immobili in cui sono situati i Data Center devono essere nella disponibilità esclusiva dell'Ente sulla base di uno dei seguenti titoli di possesso: 1. Proprietà; 2. locazione/comodato da altra PA o Demanio; 3. leasing immobiliare con possibilità di riscatto; 4. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".
IN-SA-DC-03-01	Il Data Center deve essere stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.

ID Requisito	Specifica Requisito
IN-SA-DC-04-01	Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
IN-SA-DC-05-01	L'indice di disponibilità del singolo Data Center deve essere almeno pari al 99,98 % (come rapporto tra le ore totali di servizio del Data center e le ore di disponibilità del Data center) al netto dei fermi programmati e almeno pari al 99,6% comprendendo i fermi programmati.
IN-SA-DC-06-01	L'Amministrazione deve garantire le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
IN-SA-DC-07-01	L'Amministrazione deve garantire che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
IN-SA-DE.CM-1-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-4-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-7-01	L'Amministrazione implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
IN-SA-DE.CM-8-01	L'Amministrazione implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)
IN-SA-ID.AM-1-01	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FNCS (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
IN-SA-ID.AM-2-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
IN-SA-ID.AM-3-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
IN-SA-ID.AM-6-01	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FNCS. (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))
IN-SA-ID.GV-1-01	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)

ID Requisito	Specifica Requisito
IN-SA-ID.RA-5-01	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
IN-SA-PR.AC-1-01	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
IN-SA-PR.AC-2-01	L'Amministrazione implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
IN-SA-PR.AC-3-01	L'Amministrazione implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
IN-SA-PR.AC-4-01	L'Amministrazione implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
IN-SA-PR.AT-1-01	L'Amministrazione implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
IN-SA-PR.AT-2-01	L'Amministrazione implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
IN-SA-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
IN-SA-PR.DS-5-01	L'Amministrazione implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))
IN-SA-PR.DS-6-01	L'Amministrazione implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
IN-SA-PR.IP-1-01	L'Amministrazione implementa la sotto-categoria PR.IP-1 del FNCS. (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))

ID Requisito	Specifica Requisito
IN-SA-PR.IP-12-01	L'Amministrazione implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
IN-SA-PR.IP-4-01	L'Amministrazione implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
IN-SA-PR.IP-9-01	L'Amministrazione implementa la sotto-categoria PR.IP-9 del FNCS. E' stato predisposto il piano di Disaster recovery. Sono state adottate formali procedure di emergenza in caso di indisponibilità parziale dei servizi. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
IN-SA-PR.MA-1-01	L'Amministrazione implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)
IN-SA-PR.MA-2-01	L'Amministrazione implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati)
IN-SA-RC.RP-1-01	L'Amministrazione implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
IN-SA-RS.MI-3-01	L'Amministrazione implementa la sotto-categoria RS.MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)

16.2.2 Requisiti AgID Allegato B

ID Requisito	Specifica Requisito
IN-CE-01	L'Amministrazione che eroga servizi ad altre amministrazioni deve formalizzare e pubblicare le informazioni relative ai servizi tramite il CED ricorrendo ad un apposito catalogo servizi, in conformità alle best practice ITIL. Il catalogo deve essere gestito e manutenuto attraverso un processo aderente alle best practice sul service catalogue management ITIL o alle linee guida riportate dallo standard ISO/IEC 20000-2.
IN-CE-02	L'Amministrazione che eroga servizi ad altre amministrazioni deve rendere nota la capacità di elaborazione totale del CED, quella occupata, quella libera per soddisfare i propri piani di capacity e quella a disposizione di Amministrazioni ospitate. Nello specifico, per ciascuna misura, l'Amministrazione deve dichiarare: - la superficie della sala CED o l'equivalente in numero di rack o di unità rack (U); - il numero e la tipologia di server fisici o di server farm disponibili, fornendo la capacità computazionale totale ottenuta come somma di memoria RAM disponibile [in GB], somma di CPU/Core e vCore, MIPs per gli apparati Mainframe, storage [in TB].
IN-RE-01	L'Amministrazione deve determinare con frequenza annuale l'efficienza energetica del proprio Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura del DC e quella sostenuta per gli apparati.
IN-RE-02	L'Amministrazione deve avere adottato formalmente procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001)
IN-SA-DC-08-01	L'Amministrazione deve garantire che il sistema di raffreddamento riesce a mantenere la temperatura sotto controllo anche durante la perdita dell'alimentazione elettrica principale.
IN-CE-03	La capacità elaborativa del CED deve essere gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.
IN-SA-DC-01-01	L'Amministrazione garantisce il presidio operativo del Data Center 24/7/365.
IN-SA-DC-02-01	L'Amministrazione deve dimostrare che gli immobili in cui sono situati i Data Center devono essere nella disponibilità esclusiva dell'Ente sulla base di uno dei seguenti titoli di possesso: 1. Proprietà; 2. locazione/comodato da altra PA o Demanio; 3. leasing immobiliare con possibilità di riscatto; 4. locazione o possesso da privato con contratti di tipo "rent to buy" o "vendita con patto di riservato dominio".
IN-SA-DC-03-01	Il Data Center deve essere stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.
IN-SA-DC-04-01	Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
IN-SA-DC-05-01	L'indice di disponibilità del singolo Data Center deve essere almeno pari al 99,98 % (come rapporto tra le ore totali di servizio del Data center e le ore di disponibilità del Data center) al netto dei fermi programmati e almeno pari al 99,6% comprendendo i fermi programmati.
IN-SA-DC-06-01	L'Amministrazione deve garantire le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
IN-SA-DC-07-01	L'Amministrazione deve garantire che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).
IN-SA-DE.CM-1-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-4-01	L'Amministrazione implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
IN-SA-DE.CM-7-01	L'Amministrazione implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
IN-SA-DE.CM-8-01	L'Amministrazione implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)

IN-SA-ID.AM-1-01	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FNCS (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
IN-SA-ID.AM-2-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
IN-SA-ID.AM-3-01	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FNCS (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
IN-SA-ID.AM-6-01	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FNCS. (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))
IN-SA-ID.GV-1-01	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)
IN-SA-ID.RA-5-01	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
IN-SA-PR.AC-1-01	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
IN-SA-PR.AC-2-01	L'Amministrazione implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
IN-SA-PR.AC-3-01	L'Amministrazione implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
IN-SA-PR.AC-4-01	L'Amministrazione implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
IN-SA-PR.AT-1-01	L'Amministrazione implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
IN-SA-PR.AT-2-01	L'Amministrazione implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
IN-SA-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
IN-SA-PR.DS-5-01	L'Amministrazione implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))
IN-SA-PR.DS-6-01	L'Amministrazione implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
IN-SA-PR.IP-1-01	L'Amministrazione implementa la sotto-categoria PR.IP-1 del FNCS. (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))
IN-SA-PR.IP-12-01	L'Amministrazione implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
IN-SA-PR.IP-4-01	L'Amministrazione implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
IN-SA-PR.IP-9-01	L'Amministrazione implementa la sotto-categoria PR.IP-9 del FNCS. E' stato predisposto il piano di Disaster recovery. Sono state adottate formali procedure di emergenza in caso di indisponibilità parziale dei servizi. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
IN-SA-PR.MA-1-01	L'Amministrazione implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)

IN-SA-PR.MA-2-01	L'Amministrazione implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati)
IN-SA-RC.RP-1-01	L'Amministrazione implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
IN-SA-RS.MI-3-01	L'Amministrazione implementa la sotto-categoria RS.MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)
SC-IP-01	L'ambiente cloud del servizio deve essere accessibile tramite delle API per la gestione remota. Le API esposte devono consentire l'implementazione di automatismi per la gestione remota del ciclo di vita del servizio cloud qualificato. In aggiunta, deve essere prevista la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-02	Per tutte le API esposte dal servizio cloud deve essere dichiarata l'eventuale conformità al Modello di interoperabilità emanato da AgID. Il Modello è descritto dalle linee guida riportate nella circolare AgID, n. 1 del 9 settembre 2020 e i relativi allegati, e dalle ssm. Qualora le API esposte siano conformi, devono essere condivise le specifiche dell'API in formato machine readable compatibile con le indicazioni del modello d'interoperabilità (e.g. OpenAPI3 per le API REST, WSDL per le API SOAP).
SC-IP-03	I servizi SaaS devono esporre opportune API di tipo SOAP e/o REST associate alle funzionalità applicative. Tali API devono prevedere la retrocompatibilità delle diverse versioni delle API con la versione disponibile al momento della formalizzazione del contratto con l'Amministrazione acquirente.
SC-IP-04	Il servizio cloud deve garantire la disponibilità di funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati garantendo l'utilizzo di formati open non proprietari.
SC-PS-01	Il servizio cloud deve garantire le seguenti caratteristiche come da indicazioni NIST SP 800-145 e ISO/IEC 17788:2014: 1) Self-Service provisioning: all'utente deve essere garantito di poter provvedere alla fornitura delle risorse informatiche secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Le richieste di risorse computazionali inerenti al servizio cloud oggetto di qualificazione (o informatiche) devono essere fornite unilateralmente, senza la verifica o l'approvazione del fornitore. 2) Accesso alla rete: per il servizio cloud oggetto di qualificazione devono essere offerte opzioni multiple di connettività alla rete e una di queste deve essere obbligatoriamente basata su rete pubblica (i.e. internet). 3) Pool di risorse: le risorse informatiche relative al servizio oggetto di qualificazione devono essere offerte in un pool, in modo da servire più utenti tramite un modello multi- tenant con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda degli utenti. 4) Elasticità rapida: deve essere supportato il provisioning e de-provisioning del servizio cloud oggetto di qualificazione. 5) Servizio misurabile: la fornitura a consumo del servizio cloud oggetto di qualificazione deve essere tale che l'utilizzo possa essere monitorato, controllato, segnalato e fatturato; 6) Multi-tenant: le risorse fisiche o virtuali relative al servizio oggetto di qualificazione devono essere allocate in modo tale che più tenant e relative computations e dati siano isolati e inaccessibili l'uno dall'altro.
SC-PS-02	In merito alla scalabilità del servizio cloud, devono essere gestiti e dichiarati i seguenti aspetti: - il meccanismo di scalabilità offerto (automatico e configurabile, nativo, manuale); - la tipologia (orizzontale e/o verticale); - condizione massime di carico sopportabili dal servizio (numero di utenti concorrenti e/o volume di richieste processabili); - le modalità di configurazione (sulla base di metriche di monitoraggio, pianificato nel tempo); - i tempi minimi di reazione del servizio alla richiesta di nuove risorse (i.e. attivazione di nuove risorse). In aggiunta, il fornitore rende disponibili informazioni trasparenti in merito ad eventuali ulteriori funzionalità accessorie disponibili per il servizio e configurabili dall'Amministrazione acquirente per gestire la scalabilità ed ottenere parametri migliori.
SC-QU-01	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione della qualità in conformità allo standard ISO/IEC 9001.
SC-QU-02	Per l'erogazione del servizio cloud, deve essere stato formalmente adottato dal fornitore un sistema di gestione dei servizi IT in conformità allo standard ISO/IEC 20000.

SC-QU-03	Per il servizio cloud devono essere garantite attività di supporto ai clienti. Il servizio di supporto deve essere: (I) fornito esclusivamente in lingua italiana durante le business hours, anche in lingua inglese per le emergenze 24/7; (II) accessibile almeno tramite uno dei seguenti canali preferenziali: recapito telefonico ed e-mail. In aggiunta, deve essere messo a disposizione dell'Amministrazione Acquirente un sistema di troubleshooting, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i casi di supporto.
SC-SI-DE.CM-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
SC-SI-DE.CM-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-1 del FNCS. (Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity)
SC-SI-DE.CM-7-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-7 del FNCS. (Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati)
SC-SI-DE.CM-8-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria DE.CM-8 del FNCS. (Vengono svolte scansioni per l'identificazione di vulnerabilità)
SC-SI-ID.AM-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-1 del FNCS. (Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione)
SC-SI-ID.AM-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-2 del FNCS. (Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione)
SC-SI-ID.AM-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-3 del FNCS. (I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati)
SC-SI-ID.AM-6-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.AM-6 del FNCS. (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))
SC-SI-ID.RA-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-1 del FNCS. (Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate)
SC-SI-ID.RA-5-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria ID.RA-5 del FNCS. (Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio)
SC-SI-PR.AC-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-1 del FNCS. (Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza)
SC-SI-PR.AC-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-2 del FNCS. (L'accesso fisico alle risorse è protetto e amministrato)
SC-SI-PR.AC-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-3 del FNCS. (L'accesso remoto alle risorse è amministrato)
SC-SI-PR.AC-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AC-4 del FNCS. (I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni)
SC-SI-PR.AT-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-1 del FNCS. (Tutti gli utenti sono informati e addestrati)
SC-SI-PR.AT-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.AT-2 del FNCS. (Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità)
SC-SI-PR.DS-1-01	I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.
SC-SI-PR.DS-5-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-5 del FNCS. (Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak))

SC-SI-PR.DS-6-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.DS-6 del FNCS. (Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni)
SC-SI-PR.IP-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-1 del FNCS. (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))
SC-SI-PR.IP-12-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-12 del FNCS. (Viene sviluppato e implementato un piano di gestione delle vulnerabilità)
SC-SI-PR.IP-4-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-4 del FNCS. (I backup delle informazioni sono eseguiti, amministrati e verificati)
SC-SI-PR.IP-9-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.IP-9 del FNCS. (Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro)
SC-SI-PR.MA-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-1 del FNCS. (La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati)
SC-SI-PR.MA-2-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria PR.MA-2 del FNCS. (La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati)
SC-SI-RC.RP-1-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RC.RP-1 del FNCS. (Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity)
SC-SI-RS.MI-3-01	Per l'erogazione del servizio cloud, il fornitore implementa la sotto-categoria RS.MI-3 del FNCS. (Le nuove vulnerabilità sono mitigate o documentate come rischio accettato)

16.2.3 Requisiti ACN-Allegato A2

16.2.3.1 Requisiti Dati Ordinari

ID Requisito	Specifica Requisito
A.AA-1	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	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

ID Requisito	Specifica Requisito
ID.AM-1	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	1. Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi all'Infrastruttura digitale, sono identificati ed approvati da attori interni al soggetto
ID.AM-6	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 sotituto, 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.
PR.AT-1	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	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.

ID Requisito	Specifica Requisito
PR.DS-1	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	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	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
ID.GV-1	1. Esiste un documento aggiornato che descrive le politiche, I processi e le procedure di cybersecurity.
A.GP-1	1.Sono adottati processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2.
A.GP-2	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.

ID Requisito	Specifica Requisito
PR.AC-1	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 inguistificato 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	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	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	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

ID Requisito	Specifica Requisito
PR.IP-1	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-12	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
PR.IP-4	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.MA-2	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
RS.MI-3	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.
CE.CE-01	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.
RE.GE-01	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	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.

ID Requisito	Specifica Requisito
S.DC-01	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	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, mantenuti 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.
A.PS-1	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.
RC.RP-1	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.
ID.RA-1	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 la 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	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.
DE.CM-1	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.

ID Requisito	Specifica Requisito
DE.CM-4	1. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonchè sistemi di protezione delle postazioni teminali (Endpoint Protection Systems) 2. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.
DE.CM-8	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.
RS.AN-5	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, nonchè 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 e le respondabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2

ID Requisito	Specifica Requisito
DE.AE-3	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 nonitoraggio, 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 Medi log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.
ID.AM-1	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 quell
ID.AM-2	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 nonchè la gestione non autorizzata degli asset dell'organizzazione.
ID.AM-3	1. Tutti I flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati ed approvati da attori interni al soggetto

ID Requisito	Specifica Requisito
ID.AM-6	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.
PR.AT-1	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	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.
PS.CA-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 deprovisioning del servizio, salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.

ID Requisito	Specifica Requisito
RS.CO-1	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	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.
PR.DS-1	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-PRDS-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	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.

ID Requisito	Specifica Requisito
PR.DS-3	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	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	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	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.
DE.DP-1	1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese noteall'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).

ID Requisito	Specifica Requisito
IP.GR-1	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.
ID.GV-1	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	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.
PR.AC-1	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	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.

ID Requisito	Specifica Requisito
PR.AC-4	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	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	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).
PR.IP-1	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-12	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]

ID Requisito	Specifica Requisito
PR.IP-3	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	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 l'Indicatori minimi della qualità del Servizio"
PR.IP-9	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.
IP.IN-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]

ID Requisito	Specifica Requisito
QU.LS-1	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 (SIA). 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 (SIA) 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. Ilsoggetto 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	1. All'interno dei Service Level Agreement (SIA) 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	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 Mode); 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	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.
PR.MA-1	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.

ID Requisito	Specifica Requisito
PR.MA-2	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.
IP.PO-1	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	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]
QU.PR-1	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 doud (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 doud). 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	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 doud si avvicina o supera il budget/le soglie impostate.

ID Requisito	Specifica Requisito
QU.PR-3	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).
PR.PT-1	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	1. In relazione ai piani previsti dalla sottocategoria 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.
QU.SE-1	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	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	1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).

ID Requisito	Specifica Requisito
QU.SE-4	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 1P.GR-01.
RC.RP-1	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.
RS.RP-1	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.
ID.RA-1	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	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.
PS.SC-1	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).

ID Requisito	Specifica Requisito
DE.CM-1	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	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.
ID.SC-1	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

16.2.3.2 Requisiti Dati Critici

ID Requisito	Specifica Requisito
RS-AN-5	1. Gli esiti delle valutazioni di cui alla sottoocategoria DE.AE-3 e del 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, nonchè 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

ID Requisito	Specifica Requisito
DE.AE-3	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
ID.AM-2	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, nonchè gestione non autorizzata degli asset dell'organizzazione
ID.AM-6	1. 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. 2. 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. 3. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale, 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
A.BC-3	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

ID Requisito	Specifica Requisito
RS.CO-1	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	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.
PR.DS-2	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	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	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
DE.DP-1	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.
ID.GV-1	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 Requisito	Specifica Requisito
ID.GV-4	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.
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contentente 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	3. È definito un perimetro di sicurezza tra le aree amministrative e le aree di data storage e processing
PR.AC-3	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	4. Esiste un documento aggiornato di dettaglio recante I processi di cui al punto 1
PR.AC-5	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	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
PR.IP-3	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	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.

ID Requisito	Specifica Requisito
PR.IP-9	1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dall'Infrastruttura digitale 2. Esiste un documento aggiornato di dettaglio contenente I piani di continuità operativa, nonchè 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.
PR.MA-1	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	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.
A.DC-1	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.
PR.PT-1	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

ID Requisito	Specifica Requisito
PR.PT-5	1. In relazione ai piani previsti dalla sottocategoria PR.IP-9: a. sono adottate architetture ridondate di rete, di connettività, nonchè 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
RC.RP-1	2. Il piano di ripristino viene testato su base semestrale nell'ambito di due esercitazini annuali
RS.RP-1	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, nonchè 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.
ID.RA-5	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 valuatati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-7	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 si 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
ID.SC-1	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
DE.AE-3	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

ID Requisito	Specifica Requisito
ID.AM-6	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.
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
RC.CO-3	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)
RS.CO-1	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-Discoveiy 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. E 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.

ID Requisito	Specifica Requisito
PR.DS-1	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 IDAM, 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	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]
ID.GV-1	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 governane 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
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contentente 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

ID Requisito	Specifica Requisito
PR.AC-3	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	4. Esiste un documento aggiornato di dettaglio recante I processi di cui al punto 1
PR.IP-1	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-12	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.
PR.IP-2	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	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.

ID Requisito	Specifica Requisito
PR.IP-9	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.MA-1	2. Esiste un documento aggiornato di dettaglio recante i processi 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
RS.MI-3	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.
PR.PT-5	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.
RC.RP-1	3. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

ID Requisito	Specifica Requisito
RS.RP-1	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.
ID.RA-1	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	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 DECM-8; c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-1	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 PRAC, PR.DS, PRA P e PR.MA e concorrono al rispetto delle politiche di cui alla categoria IDAM, ID.GV, ID.SC, PR.AC e PR.DS. 7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono 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.

ID Requisito	Specifica Requisito
DE.CM-4	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 PRAC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie IDAM, ID.GV, IDSC, PRAC e PRDS. 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	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 le 2 sono aggiornati, mantenuti e ben configurai, 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, PRAC e PRDS. 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	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration teste 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 teste vulnerability assessment previsti. 4. Esiste un registro aggiornato dei penetration teste vulnerability assessment eseguiti corredato dalla relativa documentazione.
ID.SC-1	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 Requisito	Specifica Requisito
ID.SC-2	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	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	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.

16.2.3.3 Requisiti Dati Strategici

ID Requisito	Specifica Requisito
DE.AE-3	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.
ID.AM-6	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):
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
A.BC-4	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
RC.CO-3	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).
RS.CO-1	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.
PR.DS-1	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.

ID Requisito	Specifica Requisito
PR.DS-3	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	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
ID.GV-1	3. Ogni scostamento dai livello 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.
PR.AC-3	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	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	3. Con riferimento ai censimenti di cui alla categoria IDAM, 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.

ID Requisito	Specifica Requisito
PR.AC-7	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.
RC.IM-2	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.
PR.IP-1	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-11	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	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.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

ID Requisito	Specifica Requisito
PR.IP-9	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.MA-1	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	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.
PR.PT-1	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.

ID Requisito	Specifica Requisito
PR.PT-4	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	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.
RS.RP-1	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 coinvolgi mento 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.
ID.RA-1	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

ID Requisito	Specifica Requisito
DE.CM-1	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 PRMA e concorrono al rispetto delle politiche di cui alla categoria IDAM, ID.GV, IDSC, 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, lemetodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
DE.CM-4	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 l D.AM, ID.GV, I D.SC, PR.AC e PRDS. 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	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, PRIP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie ID.AM, ID.GV, l D.SC, PR.AC e PRDS. 8. Esiste un documento aggiornato che descrive, almeno: a. le politiche di sicurezza adottate in relazione ai punti S e 6; b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
ID.SC-1	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 Requisito	Specifica Requisito
ID.SC-2	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, nonchè 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 i 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	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 aggiornate di conseguenza

ID Requisito	Specifica Requisito
ID.SC-4	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.
DE.AE-3	9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett a, b, c, d.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
PR.DS-1	13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio di cloud. Il soggetto rende disponibile l'elenco all'Amministrazione
PR.DS-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-5	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.AC-3	6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione. 7. E 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	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.

ID Requisito	Specifica Requisito
PR.AC-5	3. Con riferimento ai censimenti di cui alla categoria IDAM, 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	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
RC.IM-2	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.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.MA-2	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.
PR.MA-1	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
PR.PT-1	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	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.

ID Requisito	Specifica Requisito
PR.PT-5	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.
DE.CM-7	5. Con riferimento alla sottocategoria IDAM-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
ID.SC-1	6. Esiste un documento recante I processi di cui ai punti 1 e 2.
ID.SC-2	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	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.

16.2.4 Requisiti ACN-Allegato B2

16.2.4.1 Requisiti Dati Ordinari

ID Requisito	Specifica Requisito
RS.AN-5	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, nonchè 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 e le respondabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2
DE.AE-3	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 nonitoraggio, 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 Medi log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite API.

ID Requisito	Specifica Requisito
ID.AM-1	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 quell
ID.AM-2	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 nonchè la gestione non autorizzata degli asset dell'organizzazione.
ID.AM-3	1. Tutti I flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati ed approvati da attori interni al soggetto
ID.AM-6	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.
PR.AT-1	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	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.

ID Requisito	Specifica Requisito
PS.CA-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. II 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 deprovisioning del servizio, salvo documentate limitazioni tecniche, offrendo opportuni strumenti all'Amministrazione.
RS.CO-1	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	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.

ID Requisito	Specifica Requisito
PR.DS-1	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-PRDS-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	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	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	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.

ID Requisito	Specifica Requisito
PR.DS-6	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	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.
DE.DP-1	1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese noteall'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).
IP.GR-1	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.
ID.GV-1	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	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.

ID Requisito	Specifica Requisito
PR.AC-1	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	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	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	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	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).

ID Requisito	Specifica Requisito
PR.IP-1	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-12	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]
PR.IP-3	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	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 l'Indicatori minimi della qualità del Servizio"

ID Requisito	Specifica Requisito
PR.IP-9	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.
IP.IN-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]
QU.LS-1	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 (SIA). 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 (SIA) 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. Ilsoggetto 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	1. All'interno dei Service Level Agreement (SIA) 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.

ID Requisito	Specifica Requisito
QU.LS-3	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 Mode); 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	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.
PR.MA-1	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	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.
IP.PO-1	1. Sono disponibili funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari.

ID Requisito	Specifica Requisito
IP.PO-2	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]
QU.PR-1	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 doud (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 doud). 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	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 doud si avvicina o supera il budget/le soglie impostate.
QU.PR-3	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).
PR.PT-1	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.

ID Requisito	Specifica Requisito
PR.PT-5	1. In relazione ai piani previsti dalla sottocategoria 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.
QU.SE-1	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	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	1. Il soggetto deve dichiarare la frequenza attesa di aggiornamento del servizio cloud qualificato (es. periodicità rilasci pianificati).
QU.SE-4	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 1P.GR-01.
RC.RP-1	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.
RS.RP-1	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.

ID Requisito	Specifica Requisito
ID.RA-1	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	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.
PS.SC-1	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).
DE.CM-1	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	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.
ID.SC-1	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

16.2.4.2 Requisiti Dati Critici

ID Requisito	Specifica Requisito
DE.AE-3	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
ID.AM-6	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.
PR.AT-1	3. Per ogni membro del personale del soggetto, esiste un registro aggiornato, comprensivo delle istruzioni ricevute.
RC.CO-3	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)
RS.CO-1	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-Discoveiy 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. E 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.

ID Requisito	Specifica Requisito
PR.DS-1	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 IDAM, 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. II 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	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]
ID.GV-1	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 governane 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
PR.AC-1	7. Esiste un documento aggiornato di dettaglio contententente 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	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

ID Requisito	Specifica Requisito
PR.AC-4	4. Esiste un documento aggiornato di dettaglio recante I processi di cui al punto 1
PR.IP-1	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-12	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.
PR.IP-2	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	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.

ID Requisito	Specifica Requisito
PR.IP-9	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.MA-1	2. Esiste un documento aggiornato di dettaglio recante i processi 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
RS.MI-3	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.
PR.PT-5	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.
RC.RP-1	3. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

ID Requisito	Specifica Requisito
RS.RP-1	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.
ID.RA-1	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	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 DECM-8; c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati; d. l'identificazione, l'analisi e la ponderazione del rischio
DE.CM-1	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 PRAC, PR.DS, PRA P e PR.MA e concorrono al rispetto delle politiche di cui alla categoria IDAM, ID.GV, ID.SC, PR.AC e PR.DS. 7. Gli strumenti tecnici di cui ai punti 1, 3, 4 e 5 sono 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.

ID Requisito	Specifica Requisito
DE.CM-4	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 PRAC, PR.DS, PR.IP e PR.MA e concorrono al rispetto delle politiche di cui alle categorie IDAM, ID.GV, IDSC, PRAC e PRDS. 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	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 le 2 sono aggiornati, mantenuti e ben configurai, 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, PRAC e PRDS. 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	1. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration teste 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 teste vulnerability assessment previsti. 4. Esiste un registro aggiornato dei penetration teste vulnerability assessment eseguiti corredato dalla relativa documentazione.
ID.SC-1	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. II 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 Requisito	Specifica Requisito
ID.SC-2	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	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	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.

16.2.4.3 Requisiti Dati Strategici

ID Requisito	Specifica Requisito
DE.AE-3	9. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 3 lett a, b, c, d.
PR.AT-2	3. Esiste un documento aggiornato di dettaglio recante i processi di cui ai punti 1 e 2
PR.DS-1	13. Esiste un documento aggiornato che descrive da quali sedi e infrastrutture è erogato il servizio di cloud. Il soggetto rende disponibile l'elenco all'Amministrazione
PR.DS-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-5	3. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-6	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.DS-7	2. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.AC-3	6. Le politiche e procedure sono aggiornate almeno su base annuale e rese disponibili per la consultazione, dietro specifica richiesta, dell'Amministrazione. 7. E 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	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.

ID Requisito	Specifica Requisito
PR.AC-5	3. Con riferimento ai censimenti di cui alla categoria IDAM, 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	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
RC.IM-2	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.
PR.IP-3	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 1.
PR.MA-2	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.
PR.MA-1	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
PR.PT-1	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	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.

ID Requisito	Specifica Requisito
PR.PT-5	4. Esiste un documento aggiornato di dettaglio recante i processi e le politiche di cui al punto 2 lett. a e b.
DE.CM-7	5. Con riferimento alla sottocategoria IDAM-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
ID.SC-1	6. Esiste un documento recante I processi di cui ai punti 1 e 2.
ID.SC-2	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	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.

16.2.5 Requisiti ACN-Allegato C

Requisiti per la qualificazione dei servizi Cloud per la Pubblica Amministrazione.

Servizi Cloud		
Livello	**Caratteristiche dei servizi**	**Certificazioni**
1	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.	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.
2	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.	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.
3	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	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.
Ulteriori requisiti per la qualificazione cloud di livello 4		

ID Caratteristica Specifica	Caratteristica specifica	ID Requisito	Nome	Specifica Requisito
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.

Infrastruttura		
Livello	**Livelli minimi delle infrastrutture digitali**	**Certificazioni**
1	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	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
2	Ai fini della qualificazione di livello QI2 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 critici, ai sensi dell'articolo 3 del Regolamento	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
3	Ai fini della qualificazione di livello QI3 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 strategici, ai sensi dell'articolo 3 del Regolamento	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.

Ulteriori requisiti per la qualificazione infrastruttura di livello 4				
ID Caratteristica Specifica	**Caratteristica specifica**	**ID Requisito**	**Nome**	**Specifica Requisito**
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.