Norme di Sicurezza e Adeguamento

Pieve Fissiraga, 10/06/2024

Urbi Smart / WebTec / CDAN
Qualificazione dei servizi SaaS e ottemperanza al GDPR (General Data Protection Regulation Regolamento UE 2016/679), così come disposto dal Decreto Legislativo 10 agosto 2018, n. 101

Indice

1. Inquadramento

1.1. Urbi Smart: Cloud Computing e licenza d'uso

Urbi Smart[1] è il sistema informativo gestionale e direzionale integrato, web nativo, con un'unica base dati, che ha rivoluzionato la gestione delle informazioni nella Pubblica Amministrazione.
Urbi Smart è un unico strumento di supporto per il governo del Comune e degli Enti locali, accessibile da qualsiasi dispositivo mobile e in qualsiasi momento e luogo grazie alla modalità **CLOUD COMPUTING - di seguito Cloud -** definita anche SaaS (*Software as a service*) o ASP (*Application Service Providing*), ma può essere utilizzato anche nella tradizionale forma in licenza d'uso, in modalità *on premise*.
In tale configurazione, le misure di sicurezza per l'utilizzo su elaboratori di esclusiva proprietà del cliente sono a carico di quest'ultimo e non sono applicabili le misure di sicurezza intese a disciplinare il modello di erogazione SaaS.
L'architettura web nativa - con accesso mediante qualsiasi PC con browser collegato a Internet o anche attraverso i più moderni strumenti mobile (come iPad Apple, tablet con Android oltre che iPhone, smartphone, palmari ecc.) - consente una naturale predisposizione verso il Cloud.
Urbi Smart in quanto prodotto qualificato secondo le disposizioni normative e regolamentari[1] discendenti dall'attuazione dell'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, è presente sul marketplace cloud dell'Agenzia per la Cybersicurezza Nazionale[2] e soddisfa le direttive nazionali che indirizzano la digitalizzazione della Pubblica Amministrazione verso il Cloud, disegnate nella "Strategia Cloud Italia". A tal fine:

a. tutti i servizi di PA Digitale S.p.A. afferenti alla piattaforma Urbi Smart a favore della Pubblica Amministrazione sono conformi alle previsioni della Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (ACN) n. 307 del 18 gennaio 2022 ed ai relativi Allegati;
b. come previsto dalla vigente normativa, PA Digitale si avvale di un Fornitore di Servizi Cloud (CSP), che ha dichiarato analoga conformità ai requisiti della Determinazione ACN n. 307/2022. Per la qualifica QC1 e QI1 ed è anch'esso presente sul Marketplace dell'Agenzia per la Cybersicurezza Nazionale (ACN);

I Data Center di erogazione si trovano in Italia e nessuna impresa coinvolta nei trattamenti di dati è soggetta al diritto statunitense, non trasferisce dati verso l'estero, né è soggetta ai provvedimenti governativi USA FISA Section 702 e Executive Order 1233.
Oltre alla piena conformità con la normativa nazionale, l'erogazione del servizio in cloud consente di utilizzare soluzioni ad alto profilo tecnologico e costantemente aggiornate, protette e in grado di facilitare notevolmente l'interazione con i cittadini o altri soggetti esterni, senza forti investimenti infrastrutturali e pesanti costi di gestione (ad es. acquisto di software, hardware e infrastrutture di rete, costi di personale altamente specializzato per la gestione di infrastrutture complesse necessarie per usufruire della rete ecc.). Anche a seguito di un incidente di sicurezza che ha colpito un fornitore critico, sono state adottate misure ulteriormente stringenti per garantire la continuità dei dati e il consolidamento delle operazioni di backup a tempistiche ridotte.
È possibile, perciò, avvalersi anche **di un servizio specializzato che consente il ripristino rapido e completo dei dati in caso di interruzioni impreviste dei servizi e, quindi, la continuità operativa dei propri utenti** (in linea con quanto disposto dall'art. 50 del D. Lgs. 82/2005, Codice dell'Amministrazione Digitale - CAD).
Attualmente oltre 1000 Enti utilizzano Urbi Smart in modalità Cloud e più di 100 in modalità *on premise* (licenza d'uso).
La tecnologia web rende le applicazioni Urbi Smart estremamente efficaci, comunque, anche se acquisite in modalità licenza d'uso, in quanto sono tecnologicamente predisposte per essere installate in un proprio CED o presso altra server farm ed essere aperte alla rete internet. In questo contesto Urbi Smart si presta ad essere l'unica soluzione per

[1] URBI Smart e WebTec sono marchi distintivi che appartengono in esclusiva a PA Digitale
[2] la normativa applicabile è reperibile in appendice
[2] Alla data della redazione del presente documento, il portale è raggiungibile all'URL https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

aggregazioni di Comuni, CST, Comunità Montane che vogliono erogare i servizi direttamente dalla loro server farm o struttura CED.

Il modello di erogazione del servizio, le logiche e le regole sono state disegnate sugli obiettivi del sistema Paese, per avvicinare le Amministrazioni che ripongono la loro fiducia in PA Digitale alle determinazioni vincolanti del Governo nel quadro della "Strategia Cloud Italia"[3]

1.2. WebTec: Cloud Computing

WebTec è la piattaforma **di servizi per la digitalizzazione di dati, attività e processi, sviluppata con tecnologia web**, che PA Digitale rivolge a Software House, Rivenditori, Produttori di software applicativi, Dealer, System Integrator per accompagnare i loro clienti - aziende, professionisti, associazioni di categoria, ordini professionali - verso la Digital Transformation, mantenendo una completa autonomia tecnica e di mercato nonché una gestione esclusiva del cliente.
WebTec replica, per il mondo privato, le più avanzate soluzioni di sicurezza nativa, con un'attenzione profonda ai requisiti di disponibilità, integrità e riservatezza mutuati dalle regole che PA Digitale applica al settore pubblico.
Con WebTec, gli operatori ICT possono completare la loro offerta gestionale con nuovi **servizi perfettamente integrabili con i principali ERP e soluzioni gestionali, grazie a una ricca libreria di API rest**, per assicurare con la massima semplicità un colloquio applicativo e una gestione aziendale integrata con le soluzioni già in uso.
L'offerta dei servizi è ampia, ideata per la massima semplicità e fruibilità grazie anche al pannello di gestione che consente l'attivazione di servizi e funzioni: **fattura elettronica** (*PA Digitale è soggetto accreditato SDI*), **gestore documentale e conservazione digitale a norma con workflow integrato e firma digitale, workflow processuale, servizi di integrazione con l'Agenzia delle Entrate, quadratura cassetto fiscale, gestione strutturata delle PEC, web mail, gestione pratiche, agenda mobile, prenotazioni on line degli appuntamenti, servizi di *collaboration & communication* per la condivisione di dati e documenti con clienti/associati, gestione corrispondenza, gestione del credito**.
Grazie al pannello di attivazione, accessibile anche in mobilità, è **sempre garantita quindi la possibilità di attivare nuove funzioni/componenti applicative e comporre così la proposta di servizi sulla base delle reali esigenze del cliente**.
WebTec è un **sistema unico** in cui le informazioni si arricchiscono pur garantendo **l'unicità del dato** e dunque, senza duplicazione delle informazioni all'interno del DB dell'utente finale.
Tutti i servizi sono fruibili in totale mobilità e in cloud: il 100% delle funzioni è utilizzabile, per tutto il sistema e per qualsiasi utente, da un qualsiasi luogo e con qualsiasi device, ottenendo così una totale mobilità. I servizi WebTec sono quindi disponibili 24 ore su 24, 365 giorni all'anno e prevedono aggiornamenti e **backup "a caldo", senza alcun costo infrastrutturale e di gestione.**
Gli oltre 300.000 utenti finali e 70.000.000 di fatture elettroniche gestite ogni anno, per esempio, testimoniano la solidità del sistema che rende i dealer veri protagonisti dell'innovazione digitale.

1.3. Servizio di Conservazione Digitale a Norma CDAN

Il Servizio di **Conservazione Digitale a Norma** (**CDAN)** di PA Digitale, preposto alla conservazione dei documenti informatici dei Clienti, è stato **realizzato con le tecnologie più innovative** e **in conformità alle regole tecniche di cui all'art. 71 del Codice dell'Amministrazione Digitale** (CAD), la cui rispondenza è requisito indispensabile ed essenziale per la corretta conservazione dei documenti informatici.
Il servizio CDAN assicura la conservazione digitale dei documenti informatici secondo le vigenti disposizioni di legge, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità e mantenendo così inalterato nel tempo **il valore legale** dei documenti conservati.
Grazie ai numerosi automatismi e all'integrazione nativa con le applicazioni Urbi Smart e WebTec, la conservazione digitale a norma garantisce la **massima semplicità di gestione funzionalità immediate e una grafica piacevole**

[3] https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf

e intuitiva. Tutti gli accessi al sistema, sia per gli utenti sia per le operazioni automatizzate di conservazione, avvengono in totale sicurezza tramite l'utilizzo di canali di comunicazione sicuri.
CDAN è erogato in modalità Cloud Computing come SaaS (Software as a Service) per i Clienti del Mercato Pubblico e Privato ed è conforme alle recenti *Linee guida sulla formazione, gestione e conservazione dei documenti informatici e relativi allegati* pubblicate da AgID. Il Servizio di Conservazione Digitale a Norma CDAN applica quanto previsto dal *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* e dai relativi Allegati A e B.
Anche in questo caso, a fronte della stringente disciplina dettata dal legislatore nazionale ed europeo, i livelli di sicurezza applicati sia riguardo allo strato applicativo che a quello infrastrutturale sono definiti sulla base delle più stringenti norme del settore pubblico.

1.4. Cloud: vantaggi

Oltre alla possibilità di accedere ovunque alle applicazioni, l'utilizzo delle soluzioni erogate da PA Digitale in modalità Cloud (Urbi Smart, WebTec e CDAN) consente di avere molti vantaggi:

- Nessuna necessità di competenza informatica per la gestione di hardware, software e degli archivi.
- Nessun limite connesso alla necessità di dimensionamento del sistema: non occorre infatti stabilire a priori il dimensionamento dell'hardware, dato che, anche al crescere delle esigenze occorre esclusivamente aggiungere i posti di lavoro utente necessari.
- Nessun vincolo hardware e software.
- Totale eliminazione della responsabilità di archiviazione dei dati.
- Nessun vincolo contrattuale per l'eventuale cambio di fornitore.
- Estrema scalabilità.
- Aggiornamenti del software applicativo immediatamente disponibili.

2. Le Certificazioni di PA Digitale

La modalità di applicazione di quanto descritto nel presente documento è governata da un sistema di gestione integrato, articolato coerente con il contesto interno ed esterno, con riferimenti espliciti alla cornice normativa nazionale ed europea. Le politiche, le Procedure Operative Interne e le Istruzioni di Lavoro previste dal Sistema di Gestione Integrato sono conformi alle norme di standardizzazione ISO di riferimento.
Le certificazioni rappresentano l'espressa volontà di PA Digitale di dimostrare la propria responsabilità nel processo operativo, aderendo a stringenti vincoli contenuti nelle clausole e nei controlli delle norme di standardizzazione quale espressione del dovere di diligenza, correttezza e buona fede e riferimento, nel dovere di protezione, alle migliori pratiche generalmente riconosciute.
Il sistema integrato è sottoposto al processo di certificazione ad opera di un soggetto terzo indipendente, accreditato da Accredia[4] per l'ambito *Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il Mercato Privato, erogati in modalità SaaS oppure erogati con installazione in locale (on premise). Erogazione di servizi professionali connessi ai prodotti software per la Pubblica Amministrazione. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.*
Le Norme tecniche nazionali e internazionali cui PA Digitale attualmente aderisce sono pubblicate sul sito istituzionale di PA Digitale e raggiungibili nella loro versione più aggiornata al link https://www.padigitale.it/certificazioni/ e, alla data della pubblicazione del presente documento, sono:

- UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (esteso alle Linee Guida: ISO/IEC 27017:2015, ISO/IEC 27018:2019 e

[4] Accredia è l'Ente Unico nazionale di accreditamento designato dal Governo italiano, in applicazione del Regolamento europeo 765/2008, ad attestare la competenza e l'imparzialità degli organismi di certificazione, ispezione, verifica e validazione, e dei laboratori di prova e taratura. Accredia è un'associazione riconosciuta che opera senza scopo di lucro, sotto la vigilanza del Ministero delle Imprese e del Made in Italy.

ISO/IEC 27035:2023). Il processo di certificazione ha visto coinvolti i suddetti servizi su più livelli di sicurezza, da quello logico a quello fisico e organizzativo
- UNI EN ISO 22301:2019 - Sicurezza e resilienza - Sistemi di gestione per la continuità operativa
- UNI CEI ISO/IEC 20000-1:2020 - Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio
- UNI ISO 45001:2018 - Sistemi di gestione per la salute e sicurezza sul lavoro - Requisiti e guida per l'uso
- UNI ISO 37001:2016 - Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo

I Sistemi di Gestione sono integrati con la Politica Aziendale in Materia di Trattamento e Protezione dei Dati Personali pubblicata sul sito istituzionale al link https://www.padigitale.it/privacy/.

PA Digitale eroga il Servizio di Conservazione Digitale certificato in conformità:
- alla Norma UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti
- alla Norma ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements (esteso alle Linee Guida: ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27035:2023)
- alla Norma UNI EN ISO 22301:2019 - Sicurezza e resilienza - Sistemi di gestione per la continuità operativa – Requisiti
- alla Norma UNI CEI ISO/IEC 20000-1:2020 - Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio
- alla Norma UNI ISO 45001:2018 - Sistemi di gestione per la salute e sicurezza sul lavoro - Requisiti e guida per l'uso
- alla Norma UNI ISO 37001:2016 - Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo
- Alla norma ETSI EN 319 401 V2.3.1 (2021-05) - *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* e norme richiamate dalla normativa specifica sulla Conservazione Digitale a Norma e più in generale dei servizi Trusted (es.: Aggregazione SPID)
- ai requisiti individuati il servizio di "Conservatore di documenti informatici ai sensi dell'art. 29, comma 1, del D.Lgs. 7 marzo 2005, n. 82" e ss.mm.ii, tra cui si citano (a titolo esemplificativo e non esaustivo) le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" (Agid Determinazioni 407/2020 e 371/2021, con applicazione dal 1° gennaio 2022) e il "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*" (Agid Determinazione 445/2021, in vigore dal 1° gennaio 2022).

Ulteriori qualificazioni ricevute e riferimenti:
- Il Servizio di Conservazione Digitale a Norma CDAN risulta qualificato presso AgID dal 14/02/2022 mediante l'avvenuta iscrizione al Marketplace dei servizi di conservazione della società PA Digitale S.p.A. ai sensi dell'articolo 34 comma 1-bis lettera b) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell'amministrazione digitale (CAD).
  La qualificazione è consultabile al link: https://conservatoriqualificati.agid.gov.it/?page_id=276.
- I servizi SaaS Urbi Smart e CDAN sono conformi alle Circolari AgID n. 2 e 3 del 9 aprile 2018 e a quanto previsto dall'Agenzia per la Cybersicurezza Nazionale. Entrambi i servizi sono pubblicati sul Marketplace dell'Agenzia per la Cybersicurezza Nazionale consultabile al link https://www.acn.gov.it/portale/w/sa-494 e https://www.acn.gov.it/portale/w/sa-1530.
- PA Digitale adotta un Codice Etico e un Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01, disponibili in consultazione sul sito istituzionale www.padigitale.it.
- PA Digitale ha ottenuto un punteggio di "**++" (tra i più alti degli operatori di settore) nel rating di legalità pubblicato dall'Autorità Garante della Concorrenza e del Mercato "AGCM". L'Elenco delle imprese con rating di legalità aggiornato e consultabile è reso disponibile dall'AGCM sul proprio sito al link https://www.agcm.it/competenze/rating-di-legalita/rating-elenco-imprese.

3. Ottemperanza al Regolamento UE 2016 / 679 (GDPR) e relative misure di sicurezza (art. 32)

PA Digitale garantisce il rispetto del Regolamento UE 2016/679 (GDPR) e adotta tutte le misure necessarie per ottemperare a quanto previsto dall'art. 32 dello stesso Regolamento.
Le misure di seguito dettagliate rappresentano l'esplicitazione degli obiettivi di sicurezza delle informazioni riguardo ai requisiti di disponibilità, integrità e riservatezza che PA Digitale e i soggetti – definiti "ulteriori responsabili" ai sensi dell'articolo 28 del GDPR, sono tenuti ad attuare sulla base delle sistematiche attività di valutazione e gestione del rischio.
Per i clienti che usufruiscono delle soluzioni Urbi Smart e WebTec - erogate in modalità Cloud - sono valide le misure descritte in ciascuno dei capitoli seguenti.
Per i clienti che usufruiscono della soluzione Urbi Smart erogata in modalità *on premise* (licenza d'uso) sono valide le misure descritte in ciascuno dei capitoli seguenti (fatta eccezione per l'intero punto 4 e per il paragrafo 6.2).
Infine, i clienti che usufruiscono della soluzione CDAN riterranno valide tutte le misure seguenti, eccetto che per alcuni paragrafi al punto 5, essendo CDAN una soluzione integrata con Urbi Smart e WebTec, ne eredita per queste parti le relative misure di sicurezza), per il paragrafo 6.2.
Il rafforzamento dei processi di comunicazione verso i titolari, pubblici e privati e le misure adottate, che si identificano in quelle esistenti per gli operatori di servizi essenziali di cui al Decreto-Legge 105/2019, assieme a tutta la catena di fornitura dei servizi in cloud rendono la soluzione di PA Digitale **unica sul mercato**.

4. Sicurezza dei dati, continuità operativa, Security Operation Center, verifiche di conformità attraverso audit e test.

L'intera catena della fornitura dei servizi per la Pubblica Amministrazione è regolata da provvedimenti amministrativi vincolanti, che rientrano oggi nella competenza della Presidenza del Consiglio dei Ministri – Agenzia per la Cybersicurezza Nazionale, ed esercita la vigilanza sui soggetti che erogano servizi cloud per la Pubblica Amministrazione.
Principio generale della fornitura dei servizi cloud erogati da PA Digitale a favore dei propri clienti è la garanzia dei processi di sicurezza in fase iniziale e lungo tutto il ciclo di vita, sulla base del processo di gestione del rischio conforme alla metodologia definita, coerente con i principi dello standard ISO 27005.
In aggiunta, PA Digitale **ha volontariamente adottato il modello operativo esistente per gli Operatori di Servizi Essenziali, di cui alle previsioni del Decreto-Legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 105 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica" e con espresso richiamo alle misure di sicurezza di cui al DPCM 14 aprile 2021, n. 81 "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza".**
Con questo approccio, PA Digitale anticipa e rafforza i principi di attuazione della Direttiva UE 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
PA Digitale, per quanto attiene nello specifico alle misure di sicurezza implementate, richiama l'allegato I al presente documento.
PA Digitale eroga i servizi Cloud - riportati ai punti 1.1, 1.2 e 1.3 - attraverso un Data Center appartenente ad un cloud services provider certificato per l'erogazione di servizi cloud per la Pubblica Amministrazione, garantendo in tal senso la continuità del processo di accreditamento e qualificazione.
In base a tale principio, il Cloud Services Provider per la soluzione IaaS è, tenuto all'attuazione delle misure di sicurezza stabilite negli allegati tecnici alla Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza, ed è pertanto un sub-appaltatore, designato in qualità di sub-responsabile del trattamento ai fini dell'art. 28 GDPR. Le istruzioni documentate impartite al sub-responsabile sono parte integrante dell'accordo di trattamento.

Il fornitore dei servizi cloud ha la propria server farm in due data center, le cui indicazioni e caratteristiche sono indicate in Allegato II.

Ai fini della garanzia di continuità operativa, sia PA Digitale S.p.A. che il sub-fornitore dell'infrastruttura IaaS in cloud sono certificati secondo la norma di standardizzazione ISO 22301:2019 e definiscono un piano di continuità operativa in base al vigente standard internazionale ISO/IEC 27001:2022 e alle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, in cui le apparecchiature per la trasmissione dei dati e le architetture hardware/software preposte all'erogazione dei servizi sono poste in condizioni di massima **sicurezza applicativa e fisica** (sistemi antintrusione, sistemi antincendio, controllo accessi, telesorveglianza ai piani; ridondanza dei sistemi elettrici e di refrigerazione), **informatica e logica** (sistemi antintrusione).

PA Digitale applica, sia sulla rete, sia sui data center che sulle componenti applicative, un presidio di monitoraggio e controllo, mediante un **Security Operation Center**, operativo 24 ore su 24, 7 giorni su 7, sull'intero arco annuo, con requisiti disegnati in analogia con quelli definiti per gli Enti che rientrano nel Perimetro della Sicurezza Cibernetica Nazionale ed in particolare, per quelli definiti negli allegati A e B al Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021 n. 81 *"Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del Decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*".

Il Security Operation Center, oltre a svolgere un'attività di presidio continuativa e fondata su procedure sottoposte a esercitazioni periodiche, garantisce la raccolta dei bollettini di minaccia (Threat intelligence) e l'adozione tempestiva dei correttivi e delle contromisure, all'emergere di elementi di vulnerabilità o a campagne di attori ostili, in collegamento con il CSIRT Nazionale presso l'Agenzia per la Cybersicurezza Nazionale e le Autorità di contrasto (CNAIPIC della Polizia di Stato).

Relativamente alla sicurezza fisica e infrastrutturale, l'Internet Data Center è dotato di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. I sistemi di backup dei dati, la misura continuativa dei livelli di continuità dei servizi, offrono agli utenti i più elevati livelli di servizio, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tali garanzie sono fondamentali e indispensabili per gli Enti, sia per rispondere agli obblighi di legge in materia di **Business Continuity** (già citato art. 50, D. Lgs. 82/2005 - CAD), sia per poter garantire il corretto e regolare svolgimento della vita di cittadini e imprese nel caso di servizi in modalità online.

Allo stato, gli obiettivi di continuità operativa sono così declinati:
Le soluzioni architetturali di Business Continuity (intra Region) adottate sono dimensionate per poter garantire una configurazione di tipo High Availability (HA) tra Data Centers della stessa Region. Inoltre, le soluzioni adottate permettono di realizzare specifiche tipologie di configurazione dell'infrastruttura tecnologica, garantendo, in base alle caratteristiche del servizio, la soddisfazione con valori di RTO (Recovery Time Objective) e di RPO (Recovery Point Objective) compresi nel seguente range:

RTO: 30 minuti
RPO: 1 minuto

(salve dipendenze esterne non governabili da PA Digitale e TIM, come provvedimenti dell'Autorità, cause di forza maggiore, vincoli di propagazione dei DNS)

La capacità di elaborazione del sistema di business continuity permette, in caso di disastro, il ripristino dell'erogazione dei servizi con prestazioni equivalenti al sito di normale operatività, in tempi inferiori rispetto al requisito minimo richiesto dal Paragrafo 3 dell'Allegato A2 – "Livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per la Pubblica Amministrazione" meglio definite al paragrafo sottostante *4.7 Servizi di backup e Business Continuity*. Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi.

Il sito primario di erogazione servizi Cloud è presso il Data Center di TIM S.p.A. in Via di Macchia Palocco 243, Acilia, Roma (RM). Il sito secondario in Alta Affidabilità è presso il Data Center di TIM S.p.A. in Pomezia, via Pontina km 29,100.

PA Digitale, nel contesto dei propri sistemi di gestione della sicurezza e continuità operativa, adotta un processo di verifica della conformità di seconda e terza parte, attraverso:

a. Audit periodici e sistematici, secondo la norma di standardizzazione ISO 19011:2018
b. Campionamento dei processi;
c. Verifica sistematica di livelli di servizio e indicatori di performance contrattuali;
d. Vulnerability assessment e penetration test, eseguiti da soggetti esperti, secondo metodologie consolidate ed internazionalmente riconosciute (Es.: OSSTM)
e. Esercitazioni, test, drills anche estese a soggetti esterni (CNAIPIC e ACN).

I rilievi di non conformità e le osservazioni sono definiti in "Piani di rientro", che sono inclusi nei riesami periodici della direzione e nell'applicazione delle misure di rimedio contrattuale previste per i correttivi di esecuzione

4.1. Sicurezza ed affidabilità della rete dati

Le reti Metropolitane per i due Data Center (sito primario e sito secondario, citati al paragrafo precedente) si basano sulla cablatura in fibra la cui banda complessiva ad alta capacità sulla rete di proprietà dello stesso CSP con possibilità di ampliamento immediato senza modifiche infrastrutturali. Il collegamento verso la rete pubblica internet viene garantito attraverso router di backbone con attestati i link di diversi operatori. Il protocollo di routing BGPV4, costantemente gestito sui router di backbone, decide le destinazioni selezionando il carrier con la miglior qualità di servizio da e verso specifiche aree geografiche. In caso di disservizio di uno dei carrier, il BGP provvede automaticamente a instradare tutto il traffico verso l'operatore funzionante e, se necessario, anche transitando per la connettività attestata sul sito secondario rispetto al Data Center che sta erogando il servizio.
I due Data Center sono connessi tra di loro da una dorsale in fibra, permettendone la gestione come fosse un "unico" Data Center distribuito ma segmentato in logica di security e per aumentare i livelli di controllo interno. Il sistema di controllo degli accessi prevede una postazione di guardiania che identifica il personale che richiede accesso e fornisce badge che consente l'accesso alle sole aree di pertinenza.

4.2. Infrastruttura di sistema

L'**architettura del Data Center** è basata su componenti le cui principali caratteristiche sono:

- utilizzo di sole componenti di classe Enterprise;
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità effettiva dell'infrastruttura presenta un uptime non inferiore al 99.98%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate. Per garantire la massima disponibilità e fruibilità delle risorse atte all'erogazione dei servizi in modalità Cloud, PA Digitale monitora periodicamente le proprie risorse infrastrutturali predisponendo un Piano di Capacità/Capacity Plan con revisione minima annuale. Scopo di detto Piano è assicurare in ogni momento la capacità sufficiente per garantire il più alto livello di erogazione dei servizi in Cloud, in base alle attuali e future esigenze di business del mercato. Il Piano viene inoltre aggiornato in seguito a cambiamenti significativi del personale, dell'organizzazione o delle infrastrutture.

4.3. Sottosistema di virtualizzazione

I servizi sono erogati da un cluster di sistemi ad alta affidabilità VMware Enterprise.
La soluzione prescelta è di Private Cloud in conformità ai più alti requisiti di esclusiva delle risorse fisiche, logiche e computazionali. Alcune delle caratteristiche salienti:

- Vmotion: consente di migrare real time le VM tra host fisico a un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

4.4. Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su **SAN ad alte prestazioni dedicate al servizio**.
La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hardware senza completo fermo del sistema.
Le garanzie:

- **alta affidabilità dei componenti fisici**, tutti i componenti sono ridondati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- **scalabilità verticale e orizzontale dell'infrastruttura,** che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

4.5. Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall, modellata su disegno attuato dai principali organismi di sicurezza nazionale, è implementata utilizzando **due firewall in cluster HA**, per la gestione dell'accesso internet e per la gestione della DMZ e LAN interna, cui è anteposta una soluzione di protezione mission-critical per la protezione di infrastrutture e contenuti senza pregiudicare la fruibilità dell'esperienza utente.
I server applicativi utilizzano **VLAN** per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.
L'infrastruttura dispone di **sonde IPS** (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service), di sonde antivirus per l'analisi di tutto il traffico web e per prevenire l'eventuale infezione causata da malware.
La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di password a criptazione forte.
L'accesso all'IDC da parte di PA Digitale ai sistemi per scopi di amministrazione avviene attraverso connessioni **VPN** autenticate attraverso username/password e certificati digitali, oppure tramite VPN site 2 site IPSEC configurata direttamente fra i firewall di PAD e del sito primario. In quest'ultimo caso, è prevista un'ulteriore abilitazione specifica a livello di firewall.
Il servizio di monitoraggio di sicurezza è garantito dalla società TIM S.p.A. attraverso il proprio Security Operation Center, che effettua attività di monitoraggio, rilevamento e analisi incidenti, contenimento ed eventuale supporto al ripristino, oltre ad assicurare le funzioni di interfaccia con le competenti Autorità in caso di eventi.

4.6. Politiche di backup

Le politiche di backup adottate prevedono la gestione di tutti i dati relativi a Urbi Smart, WebTec e CDAN: database, documenti e componenti applicative. I backup hanno frequenza giornaliera e retention/storico di 30 giorni. I job di backup, con modalità "Full backup" e "incremental backup" concomitanti costituiscono la **Catena di backup**, la cui esecuzione non ha impatti sull'erogazione dei servizi; i backup dei database avvengono a caldo sul nodo del cluster "slave".
Per quanto descritto e a salvaguardia di una maggiore integrità dei dati, TIM Flex Backup esegue automaticamente ogni settimana un full backup per ogni job schedulato, a prescindere dalla policy impostata, creando in questo modo catene corte della durata massima di 1 settimana (7 restore point). Nel caso di retention a lunga scadenza si avranno diverse catene, di 1 settimana ciascuna, per la durata prevista dalla policy.
La soluzione TIM Flex Backup si fonda su un'architettura distribuita in cui ogni livello è separato fisicamente mediante l'uso di edge di protezione (es.: firewall, vrf, contract, ecc) per un elevato livello di sicurezza.

Per ogni vm protetta, viene eseguito un backup a livello "image" ovvero dell'intera VM in termini di sistema operativo, disco dati e configurazione della memoria quindi, a differenza del backup File System, l'eventuale restore della vm non necessita di re-installare gli applicativi, di ri-configurazioni ecc.
La soluzione lavora di default in modalità Agent-Less a meno di situazioni particolari in cui si utilizzerà l'Agent e/o i Plug-in.
L'infrastruttura di backup si integra nativamente con l'Hypervisor vmware e crea l'immagine della vm da salvare mediante snapshot, utilizzando le primitive di Vmware; l'immagine viene ottimizzata e deduplicata prima del salvataggio sul target Repository (Storage di Backup presente nel Data Layer).
Durante i backup incrementali, il Change Block Tracking (CBT) individua e salva solamente i blocchi di dati che sono variati rispetto all'ultimo backup.
Ogni operazione di backup / restore, per poter essere performante ed efficace, viene parallelizzata in base ai dischi della vm ossia viene generato un processo per ogni disco di una vm ed il carico di lavoro dei componenti di backup è distribuito per tutta l'infrastruttura TIM Flex.
È altresì adottata una misura definita di "Crash-Consistency" che equivale allo stato di una macchina virtuale dopo un riavvio forzato o un'improvvisa interruzione dell'alimentazione. Ciò significa che nella stragrande maggioranza dei casi, la macchina virtuale si avvierà nuovamente senza incontrare problemi.
Per le applicazioni definite come critiche in sede di valutazione del rischio, è applicato un livello di consistenza più elevato.

4.7. Servizi di backup "Golden Copy" e Business Continuity

La strategia di backup adottata per l'adozione delle Politiche descritte al punto precedente prevede l'implementazione e l'utilizzo di piattaforma che permette:

a) Preliminare verifica dei files, con individuazione e rimozione di anomalie e vulnerabilità
b) controllo accessi multifattoriale e granularità delle politiche di controllo basate sui ruoli e token-based authentication per l'accesso al vault
c) air-gap virtuale (separazione fisica e logica)
d) la cifratura dei dati a riposo;
e) immutabilità dei dati mediante immutabilità del dato (Retention lock).

Le soluzioni adottate permettono la rigida limitazione delle possibilità di accesso e scrittura e il recupero dei dati in caso di necessità, garantendone un corretto processo di ripristino e l'identificazione dei dati necessari recuperando il supporto di backup appropriato.
Sono pianificate delle prove di ripristino dei dati in maniera randomica, che consistono nel restore di un ambiente virtuale in un'area di test e le relative verifiche di buon funzionamento. La granularità dei backup relative ai database consente il recupero a livello del singolo record a una data specifica.
Il processo di alta affidabilità, ridondata su due siti sempre attivi nella medesima "Region" consente di superare la logica del Disaster Recovery, con un continuo allineamento dei dati e la segregazione delle reti e dei sistemi, sotto il presidio dei controlli tecnici ed operativi del Security Operation Center, altamente automatizzato con il più evoluto sistema SOAR (Security Orchestration Automation Response).

5. La gestione della sicurezza e sistemi di security management per le procedure applicative – Identity Access Management e Privileged Asset Management

La gestione della sicurezza costituisce una tra le componenti più delicate nell'ambito, più generale, della gestione dei dati dei Clienti. Sia l'infrastruttura che i servizi SaaS erogati in modalità Cloud da PA Digitale sono periodicamente sottoposti ad attività di Vulnerability Assessment e Penetration Test, effettuati da un ente terzo indipendente certificato da Accredia ed in possesso di qualificazione appropriata.
Dovendo implementare un IDC per l'erogazione dei servizi di amministrazione degli enti in modalità Cloud, PA Digitale ha da tempo sviluppato e attuato una metodologia per l'analisi dei rischi legati alla sicurezza e alla sua gestione attraverso opportuni meccanismi e strumenti di controllo e di intervento.

Le scelte adottate, in linea con quanto enunciato dall'Agenzia per l'Italia Digitale e dall'Agenzia per la Cybersicurezza Nazionale in materia di sicurezza, portano a:

- controllo e monitoraggio degli accessi in modo puntuale e nel tempo;
- identificazione di eventuali anomalie;
- intervento nel minor tempo possibile per ripristinare la situazione correttamente.

Logiche sempre più stringenti, in progressivo avvicinamento al modello "Zero Trust" (NIST-800.207), convergono verso l'adozione di misure di rigore, quali:

a. l'adozione di sistemi di autenticazione multifattoriale, inizialmente a scelta del cliente, per agevolare una transizione a basso impatto sulle Amministrazioni e poi, progressivamente, resa obbligatoria su tutti gli utenti;
b. un rigoroso controllo delle utenze di amministrazione o con privilegi elevati e delle persone;
c. la segregazione dei ruoli;
d. la microsegmentazione delle reti;
e. l'identificazione e la riconoscibilità degli asset abilitati ad operazioni critiche.

5.1. Principi applicabili al legittimo trattamento dei dati

Per soddisfare i requisiti di sicurezza, le soluzioni Urbi Smart, WebTec e CDAN osservano principi applicabili al legittimo trattamento dei dati (con particolare riguardo verso le Informazioni Personali Identificabili - PII), supportando una serie di servizi e di dispositivi atti a implementare funzioni di autenticazione, autorizzazione e crittografia. Tali servizi e dispositivi risultano adeguati alla normativa UE 2016/679 in vigore dal 25.05.2018, così come disposto in Italia dal Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)*".

L'**autenticazione** prevede che gli utenti si debbano identificare con una serie nota di credenziali, ad esempio nome utente e password. Per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.

Per **autorizzazione**, invece, si intende l'assegnazione di determinati livelli di accesso al sistema, che identificano specifiche capacità operative sul sistema medesimo da parte dell'utente correttamente identificato.

L'attribuzione dei privilegi degli utenti, intesi come regole sia di autenticazione che di autorizzazione, è esclusivamente demandata all'Amministratore applicativo. Quest'ultimo può decidere se applicare su altri utenti i privilegi che regolano le policy di sicurezza, di accesso, visibilità e gestione dei dati.

La **sicurezza** dei dati è garantita:

- durante la fase di comunicazione client e server tramite utilizzo di protocollo https e crittografia di tipo TLS 1.2 o superiori
- nello storage all'interno del database
- durante la fase di comunicazione tra sottosistemi di infrastruttura (webserver, long run process server, dbms server, NAS) o applicativi (comunicazioni da/verso sistemi ministeriali e/o di terze parti mediante identificazione degli enti coinvolti nello scambio dei flussi informativi e degli utenti abilitati all'accesso ai servizi anche tramite l'utilizzo di certificati digitali).

I servizi sono sottoposti a controllo costante dell'erogazione e delle prestazioni del servizio mediante strumenti di supervisione, accessibili via web dal personale abilitato.

Di seguito le caratteristiche del gestionale espresse in forma sintetica che saranno dettagliate nei paragrafi successivi.

a. Erogazione servizio tramite protocollo https
b. Accessi al software protetti da "nome utente" e "password".
c. Password di accesso "sicure".
d. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.
e. Protezione dei dati
f. Tracciabilità dei log di accesso per eventuali comunicazioni di Data Breach.
g. Tracciabilità delle variazioni ai dati del sistema

5.1.1. Erogazione servizi mediante protocollo HTTPS

I servizi di backoffice e i servizi on line di Urbi Smart, WebTec e CDAN possono essere erogati mediante protocollo HTTPS. Il protocollo HTTPS consiste nel far transitare la comunicazione tramite il protocollo HTTP all'interno di una connessione criptata dal Transport Layer Security (TLS) 1.2 o superiori. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti. Il principio che sta alla base di HTTPS è quello di avere:

- un'autenticazione del sito web visitato
- protezione della privacy
- integrità dei dati scambiati tra le parti comunicanti.

I processi di threat intelligence provvedono a sottoporre a costante monitoraggio i punti di accesso internet e a verificare aspetti reputazionali e informazioni che ruotano nelle aree del web non indicizzato (deep web) e nelle aree del web accessibili solo attraverso l'uso di software specifici e ad accesso condizionato, dove proliferano attori malevoli (dark web).

5.1.2. Accessi al software protetti da nome utente e password

Urbi Smart, WebTec e CDAN utilizzano un sistema di **autenticazione basato su sessione**. Ogni programma all'interno delle tre soluzioni verifica la validità della sessione in corso (identificata da un token di sessione) prima di fornire la pagina richiesta. Allorché la sessione sia scaduta o non sia attiva, qualsiasi richiesta viene ridirezionata al sistema di autenticazione. Il sistema di autenticazione standard prevede autenticazione basata su **Login e Password.** L'utente è identificato all'interno di una base dati da un *nome utente* e da una *password*, secondo lo schema seguente:

- login: nomeutente@identificativodb
- password: Password_Utente

Nomeutente, identificativodb e password sono gli elementi essenziali e univoci per procedere alla validazione di un utente.
Su richiesta, sono disponibili integrazioni a strumenti di autenticazione standard (es. LDAP, Active Directory) attraverso cui ricondursi a utenti censiti in Urbi Smart e WebTec.
Come già anticipato, per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.
Dal 06/05/2024 è inoltre disponibile la modalità di autenticazione a due fattori.
L'autenticazione a due o più fattori (conosciuta anche come strong authentication) è oggi il sistema di protezione più sicuro per proteggere i propri account e una maggiore possibilità di controllo da parte dell'utente proprietario dell'account. Abbina alle credenziali (login, password), l'obbligo di confermare attraverso il proprio smartphone l'operazione. Con il rilascio del 6 maggio 2024 sarà possibile accedere ad URBI Smart attraverso questa modalità previa abilitazione da parte dell'amministratore di sistema.
L'autenticazione a più fattori rappresenta un importante scudo di protezione per gli utenti che si avvalgono di servizi digitali ed è una prassi ormai molto diffusa in svariati tipi di servizio (Banche, Assicurazioni, Social network, servizi e app varie). L'autenticazione a due fattori è ad oggi la misura di sicurezza più efficace per proteggere i propri account dalla minaccia del furto d'identità e contrastare gli attacchi di phishing con cui gli hacker cercano di ottenere informazioni sui dati sensibili degli utenti.
Previo nulla osta a livello di ente da parte dell'Amministratore di Sistema, è previsto un passaggio graduale, all'autenticazione Multifattore (MFA nel periodo di tempo compreso tra il rilascio previsto per il 6 maggio e il 2 luglio 2024. Dal 3 luglio 2024 gli utenti potranno accedere solo con l'autenticazione Multifattore.

5.1.3. Password di accesso sicure

Ad ogni utente, l'Amministratore applicativo può assegnare:

1. **Data Scadenza Utente**: questa data indica la data fino alla quale l'utente è valido. **Scaduta questa data l'utente viene disattivato**. Questa data serve per consentire di attivare un utente per un certo periodo di tempo: se si lascia il campo vuoto, oppure impostato a valore infinito 31-12-9999, l'utente è sempre attivo.
2. **Password d'Ufficio**: se non diversamente specificato, l'utente è costretto a modificare la password al primo

accesso della procedura.

3. **Data Attivazione Password:** questa data (impostata di default al giorno di creazione dell'utente) indica la data di attivazione della password per l'utente. In alcuni casi può essere utile attivare gli utenti in date posteriori alla creazione dell'utente stesso.
4. **Giorni Validità Password:** indica per quanti giorni la password di un utente è valida, a partire dalla data di attivazione. Questo campo è utile per definire un periodo di validità della password all'interno del range definito tra la data attivazione e la data scadenza. L'Amministratore applicativo può decidere la policy utente alla scadenza dei giorni di validità. Le due scelte possibili sono: a) costringere l'utente a cambiare password b) disattivare l'utente.
5. **Max Giorni Non Loggato:** indica il numero massimo di giorni in cui un utente può restare attivo senza accedere a Urbi Smart e WebTec. Trascorso tale numero di giorni senza che l'utente acceda al sistema, la procedura lo disattiva in automatico.

All'atto della creazione di un nuovo utente, l'Amministratore gli attribuisce:

1. la **Password** (di default viene impostata come password d'ufficio)
2. la **Data di Scadenza Utente**
3. la **Data di Attivazione della Password** (impostata alla data del giorno) e il numero di **Giorni di Validità della Password**
4. il numero **Max Giorni Non Loggato** (se si vuole che venga disattivato l'utente che non accede a Urbi Smart e WebTec per più di un certo numero di giorni consecutivi).

Le password sono tutte crittografate La prima volta che il nuovo utente entra nella procedura deve utilizzare la password attribuita dall'amministratore. Se la password assegnatagli è una **password d'ufficio**, il sistema gli presenta in automatico la sezione per il cambio password obbligatorio: **l'utente deve inserire una nuova password compresa tra 8 e 30 caratteri (almeno 2 numeri e almeno 5 lettere dell'alfabeto ed almeno un carattere tra . ; $! - < >)**. Il Titolare può scegliere di impostare la lunghezza minima della password conformemente a quanto previsto dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni", ovvero impostando un minimo di 12 caratteri (14 per gli Amministratori di Sistema). Modificata la password può ritornare a Urbi Smart e WebTec tramite link contenuto nella maschera. Se l'utente sbaglia le credenziali per tre volte consecutive viene disabilitato e può essere riabilitato solo mediante l'intervento dell'Amministratore, che agirà sempre attraverso l'interfaccia di gestione utenti. Il numero minimo di tentativi disponibili per tentare l'accesso è settato a 3, ma l'Amministratore applicativo può decidere di aumentare questo valore massimo 9, secondo le politiche interne al cliente.

Un utente viene inoltre disabilitato se:

1. è scaduto (**Data Scadenza Utente** scaduta)
2. è stato per **MaxGiorniNonLoggato** senza accedere a Urbi Smart e WebTec (se tale valore è stato definito).

la sua password è scaduta (**Giorni Validità Password**, settato) ed è stato definito che alla scadenza l'utente debba essere disattivato.Anche in questi casi è necessario riabilitarlo tramite l'intervento dell'Amministratore, come sopra.

L'**annullamento** di un utente prevede di annullare logicamente l'utente medesimo, in modo da garantire che le credenziali di autenticazione non saranno mai più utilizzate per diversi utenti, neppure in tempi diversi. Un utente **ANNULLATO** viene ancora visualizzato nella lista degli utenti (in apposita sezione), ma non è più attivo e non è più possibile effettuare operazioni su di esso. In questo modo si garantisce che non sarà mai inserito un utente con lo stesso nome di un utente già utilizzato in precedenza (anche se annullato).

5.1.4. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.

Urbi Smart e WebTec permettono la definizione di tre tipologie di utenti in funzione della loro visibilità ed accessibilità alle varie procedure, e quindi in funzione del tipo di menù assegnato. In particolare:

1. **Utente Standard**: l'utente può entrare nell'area delle procedure abilitate e accedere di default a tutti i programmi raggiungibili in virtù del suo Profilo Primario (Visione, Gestione, Supervisore). È tuttavia possibile prevedere un ulteriore livello di autorizzazione, disabilitando l'accesso solo ad alcuni programmi.
2. **Utente Scrivania**: questo tipo di utente può accedere esclusivamente ai programmi che gli sono stati espressamente abilitati. L'utente Scrivania può accedere a Urbi Smart e WebTec solamente alle procedure che gli sono state assegnate, e la pagina di accesso proposta contiene soltanto i programmi che gli sono stati assegnati (non ha la navigazione completa dell'utente Standard).

3. **Utente Misto** (valido solo per Urbi Smart): è l'utente che è Standard per alcune procedure e Scrivania per altre. Ad esempio: un utente standard dell'anagrafe (che ha a disposizione tutte le scelte del menù anagrafico) al quale viene attivata la sola funzione di visualizzazione delle delibere o visualizzazione dei protocolli.

È possibile prevedere ulteriori autorizzazioni relative a specifiche applicazioni Urbi Smart e WebTec.
Tutti i programmi Urbi Smart e WebTec, al momento del rilascio, sono suddivisi per singole Procedure e ciascuno di essi viene rilasciato con un livello di accesso di default scelto fra tre tipologie di Programma: Programma di Visione, Programma di Gestione o Programma di Supervisore. Analogamente, eventuali Funzioni associate ai programmi stessi sono rilasciate con un valore di default fra Funzione Abilitata o Funzione Disabilitata.

Urbi Smart e WebTec prevedono la gestione delle abilitazioni organizzata a livelli:
- a livello di Procedura, relative a tutti i programmi della procedura;
- a livello di Programma, con accesso al programma, inserimento di dati, annullamento di dati, variazione di dati;
- abilitazioni all'interno del programma di particolari Funzioni.

Di conseguenza, sono previsti tre livelli di intervento per la definizione dei privilegi utente:
- associazione di uno dei Profili di Base previsti (a livello di procedura);
- abilitazione o meno dello specifico programma;
- abilitazione del programma con inibizione o meno di specifiche funzioni.

Nella tabella seguente sono evidenziate le abilitazioni di default sui programmi di una procedura in funzione dei Profili di Base di un utente:

Profilo Base	Abilitazione di default dei programmi della procedura
Visione	Solo programmi definiti come Visione
Gestione	Programmi definiti come Visione e Gestione
Supervisore	Programmi definiti come Visione, Gestione e Supervisore
Scrivania	Solo programmi esplicitamente assegnati

Controllo interventi sui soggetti
Il soggetto, sia esso una persona fisica o un soggetto giuridico, acquisisce in Urbi Smart e WebTec un'importanza elevata. Costituendo il punto centrale di indagini nell'ambito del sistema informativo ed essendo presente una sola volta come codice e relativo corredo anagrafico, necessita di una serie di controlli capillari sul trattamento delle sue informazioni. Due sono le sezioni previste per il controllo degli interventi sui soggetti: Variazione e Annullamento. Ogni variazione inerente a quello che è stato definito corredo anagrafico di un soggetto (fanno parte di questo gruppo per esempio cognome, nome, data nascita, codice fiscale) viene concessa esclusivamente se l'utente che vuole effettuare è autorizzato a compiere una Variazione e/o un Annullamento.
Gestione classi di utenti
La funzione è stata progettata per rendere più efficiente e ottimizzata la gestione delle profilazioni degli utenti. È possibile identificare una serie di utenti di riferimento (utenti di tipo classe) e permettere a tutti gli utenti collegati a una classe di ereditare le caratteristiche dell'utente capofila o di riferimento. Grazie a tale impostazione, è possibile effettuare estrazioni o applicare filtri esclusivamente a determinate classi di utenti.
Gestione stampe
La gestione dello spool delle stampe segue di pari passo la gestione degli utenti/classi utente. Ciascun utente può generare le stampe secondo le abilitazioni definite seguendo i criteri elencati nel presente paragrafo. Come per la gestione utenti, anche per la gestione delle stampe l'Amministratore applicativo ha la possibilità di sovrintendere l'intero sistema delle stampe, per mezzo di funzioni di ricerca mirata all'interno dello spool.

5.1.5. Protezione dei dati

In funzione della protezione dell'accesso ai dati, il meccanismo si fonda su un sistema di permessi basato sui ruoli definiti in pianta organica e nella gestione utenti descritta al paragrafo precedente. L'accesso ai dati avviene solo

attraverso l'applicazione; i server di database sono protetti **da un doppio sistema di firewall e da regole di routing** che non ne consentono la visibilità dall'esterno della rete.
La gestione della base dati unica relativa al singolo Ente è basata su database standard. Nel caso di utilizzo del sistema in modalità Cloud con collegamento al Data Center, il database adottato è Maria DB. In tutti i casi il sistema ne rispecchia le caratteristiche in termini tecnico-funzionali.
I database dei singoli Enti sono distinti e ad ognuno di essi è stato associato un utente/schema. Ad ogni schema non vengono concessi privilegi ulteriori che comportino l'accesso e/o la gestione di oggetti appartenenti ad altri schemi. Non esistono aree condivise tra i vari schemi.
La connessione dall'application server al database avviene attraverso un servizio di rete diverso per ogni Ente. Gli utenti di un ente, al momento dell'accesso, discriminano lo schema associato e l'autenticazione viene effettuata attraverso l'utente, lo schema e relativa password. Questi tre elementi sono indipendenti per ogni ente.

5.1.6. Tracciabilità dei log di accesso

fermo restando l'obbligo di garantire i processi di audit log per le funzioni di amministrazione di sistema, funzionali agli adempimenti di verifica di sicurezza e di tutela dei dati personali, il sistema di autenticazione basato su sessione rende implicitamente disponibile una funzione di monitoraggio attività sul sistema. Attraverso apposita tabella, infatti, possono essere memorizzate le sessioni d'uso istanziate e chiuse, i tentativi di accesso non riusciti, i rinnovi di sessione, ecc. La richiesta al Session Manager, inoltrata ogni qualvolta un utente fa una richiesta a Urbi Smart, WebTec e/o a CDAN, consente di registrare informazioni sulle operazioni eseguite con tracciamento per ogni utente, programma, evento. La logica di base con cui sono sviluppati i programmi di Urbi Smart, WebTec e CDAN fa sì che ciascuna operazione svolta dagli utenti (visualizzazione di una maschera, inserimento, modifica o rimozione di dati) avvenga tramite il richiamo di un evento che viene tracciato. Vengono difatti tracciati:
- token di sessione
- utente loggato
- Remote IP da cui è pervenuta la chiamata
- TimeStamp dell'evento
- estremi della chiamata

La struttura è in grado di memorizzare anche situazioni del tipo:
- "Non si dispone delle credenziali per procedere." @ErroreLogin (dove ErroreLogin riporta l'esatta motivazione dell'errore)
- "Errore in fase di derivazione delle credenziali per la base dati. Chiudere e riaprire il browser, quindi riprovare"
- "Sessione non valida!"
- "Sessione scaduta!"
- "Sessione con IP reimpostato, rieffettuare la login!"
- "Non si dispone delle autorizzazioni per accedere, chiudere il browser e rieffettuare la login!"
- LOGIN utente
- LOGOUT utente.

Tali funzioni concorrono alle attività del Security Operation Center e supportano le analisi di natura tecnica e di sicurezza e l'eventuale analisi forense in ipotesi di eventi suscettibili di investigazione o di violazioni di sicurezza.

5.1.7. Tracciabilità delle variazioni ai dati del sistema

Urbi Smart e WebTec sono dotati di un sistema di monitoraggio delle variazioni alla base dati. Le variazioni applicative alla base dati vengono tracciate riportando, per ogni sessione di variazione:
- grandezza variata
- utente che ha effettuato la variazione
- istanza applicativa che ha provocato la variazione
- valore precedente alla variazione
- valore successivo alla variazione.

Funzioni applicative di interrogazione consentono l'analisi del monitoraggio.

6. Erogazione servizio di assistenza remota

PA Digitale fornisce il servizio di assistenza remota attraverso uno specifico settore di Help Desk e mediante due modalità differenti:

1. collegamento da remoto mediante software di accesso a desktop remoto, incluso nel contratto di assistenza;
2. accesso da remoto, tramite l'utente "PAD_SUPPORT" (per il solo Urbi Smart), adottato solo a seguito di sottoscrizione da parte del cliente di una specifica autorizzazione formale.

6.1.1. Collegamento da remoto

Viene utilizzata questa modalità nei casi in cui l'Operatore di Help Desk, per erogare il supporto al cliente richiedente, non abbia la necessità di operare sul sistema del cliente ma solamente di guidare l'Utente e visualizzare le operazioni che quest'ultimo effettua sull'applicativo.
Il collegamento viene effettuato mediante un software di accesso a desktop remoto, leader di mercato, che garantisce la sicurezza degli utenti e delle connessioni mediante infrastruttura certificata ISO/IEC 27001 e interamente conforme alle norme HIPAA e SOC2:

- Crittografia AES a 256 bit
- Autenticazione a due fattori
- Protezione da forza bruta
- Lista bianca per utenti e IP
- Elenco dei dispositivi fidati
- Reset della password forzato.

6.1.2. Accesso mediante utente "PAD_SUPPORT"

A seguito di esplicita autorizzazione del cliente, e trasmessa via PEC, PA Digitale crea uno specifico utente e provvede alla configurazione dell'ambiente di lavoro.
Per mezzo di questa modalità, abilitata di volta in volta dal Cliente in ciascuna richiesta di assistenza, gli Operatori di Help Desk possono accedere in autonomia al database del cliente tramite uno specifico utente di sistema creato ad hoc (PAD_SUPPORT), al fine effettuare la corretta diagnostica delle problematiche segnalate. Gli Operatori di Help Desk potranno quindi effettuare le operazioni correttive direttamente "sulle" soluzioni applicative in uso dal Cliente - risolvendo dove possibile direttamente le necessità segnalate, senza la necessità che una persona che presidi l'intervento. Attraverso questa modalità si incrementa l'efficienza dei servizi di Assistenza, velocizzando i tempi di risposta e procedendo in maniera più rapida alla risoluzione delle problematiche evidenziate, nel rispetto della trasparenza così come della normativa sulla privacy, attraverso una puntuale tracciatura delle attività effettuate dagli Operatori di Help Desk. Tutte le operazioni sono infatti tracciate in uno specifico log che, al termine dell'intervento, viene firmato digitalmente, allegato al ticket di assistenza e messo a disposizione del Cliente nel caso in cui lo richieda.
Nell'eventualità che, per una specifica richiesta d'assistenza, il Cliente non voglia permettere l'utilizzo di tale funzionalità, il richiedente medesimo dovrà disabilitare il check "Assistenza tramite Backdoor in fase di inserimento del ticket", che di base è sempre valorizzato.

7. Subappalto di servizi – designazione degli ulteriori responsabili ex art. 28 GDPR

Nei casi in cui PA Digitale abbia la necessità di subappaltare una componente e/o alcune attività previste dal servizio di utilizzo di Urbi Smart e/o WebTec, dopo aver verificato i requisiti di esperienza, di professionalità, di capacità e di affidabilità del fornitore, sottoscrive con quest'ultimo un contratto formale che contiene, oltre alle clausole contrattuali, il disciplinare tecnico che regolamenta la modalità di erogazione del servizio da prestare e le misure di sicurezza da adottare per garantire la sicurezza delle informazioni e di tutti i dati trattati (con particolare riguardo verso le Informazioni Personali Identificabili - PII).

Nel caso in cui il fornitore, per espletare il proprio servizio, non sia tenuto ad effettuare alcun trattamento di dati personali, tale divieto è espressamente indicato nel contratto di servizio. Nel caso in cui il fornitore debba effettuare un trattamento di dati personali, tale fornitore viene nominato Sub-Responsabile del trattamento dei dati in outsourcing, per ciascun servizio assegnato. Nella lettera di nomina sono riportate:

- le finalità del trattamento
- i dati da trattare
- la base giuridica
- la durata del trattamento
- le indicazioni nonché le specifiche istruzioni a cui attenersi affinché tutte le operazioni di trattamento informatico e manuale dei dati personali, nei limiti delle competenze e attribuzioni del fornitore, siano effettuate nel rispetto della normativa vigente e dei regolamenti aziendali in materia di tutela dei dati personali, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento UE 2016/679 (art. 28 comma 4).

Non è previsto il subappalto di servizi per l'utilizzo di CDAN, ad eccezione della componente di data center.

Il quadro dei subappalti, che costituisce riferimento ai fini dell'accordo ex art. 28 GDPR, è contenuto nel dettaglio nell'Accordo tra Titolare e Responsabile, reso in conformità della Decisione di Esecuzione (UE) 2021/915 della Commissione.

8. La restituzione dei dati a conclusione o revoca del contratto di Urbi Smart e WebTec

All'atto della conclusione e della revoca del contratto in essere, e a seguito del pagamento dell'eventuale debito in essere, PA Digitale in qualità di Responsabile esterno del trattamento:

- permetterà al Titolare del trattamento di prelevare dai sistemi elettronici di PA Digitale gli archivi informatici tramite apposita funzione;
- è tenuta a conservare nell'IDC (Internet Data Center) i dati del Cliente per un periodo non superiore a 90 (novanta) giorni dalla data di cessazione degli Ordinativi di fornitura, per qualsiasi causa essa intervenga. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare fisicamente dall'IDC i dati e tutte le relative copie di salvataggio, con modalità di cancellazione sicura.

Tali misure si applicano ai Clienti che usufruiscano delle soluzioni Urbi Smart e WebTec in Cloud.

8.1. La restituzione dei dati a conclusione o revoca del contratto di conservazione digitale dei documenti informatici

In caso di risoluzione del Contratto i documenti informatici originariamente versati dal Cliente nel sistema di Conservazione CDAN saranno a quest'ultimo restituiti nel loro formato originale, fatto salvo il caso che i suddetti documenti abbiano subito una conversione di formato per sopperire all'obsolescenza del formato originario; in quest'ultimo caso saranno restituiti nel formato convertito. Contestualmente, saranno restituiti anche i metadati associati ai documenti informatici originariamente forniti dal Cliente.
PA Digitale, in tutti i casi di risoluzione del Contratto, consentirà al Cliente di recuperare i propri documenti informatici, entro e non oltre 180 (centoottanta) giorni dalla cessazione del Contratto, dopo che questi avrà corrisposto a PA Digitale tutti gli importi contrattualmente dovuti. I documenti informatici dovranno essere prelevati dal Cliente secondo le modalità stabilite nel Manuale del sistema di Conservazione e dal Contratto - quindi non incombe su PA Digitale alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare dal proprio IDC i documenti informatici e gli annessi metadati di cui il Cliente è titolare (e tutte le relative copie di salvataggio), con modalità di cancellazione sicura.

ALLEGATO I

MISURE DI SICUREZZA IMPLEMENTATE E LIVELLI DI SERVIZIO

SUB 1 – REQUISITI DI CERTIFICAZIONE

REQUISITO: Per l'esercizio delle attività di CSP qualificato per l'erogazione di servizi cloud per la pubblica amministrazione sono richieste certificazioni specifiche su standard ISO (Determina ACN 307/2022)	PA DIGITALE	CLOUD SERVICES PROVIDER TIM/NOOVLE	PROVIDER DEI SERVIZI DI ASSISTENZA	SERVIZI SOC
ISO 9001:2015	Sì	Sì	Non richiesto	Non richiesto
ISO/IEC 27001:2013 oppure 27001:2022, con est. 27017:2015 e 27018.2019	Sì	Sì	Non richiesto	Non richiesto
Per servizi critici: ISO 22301:2019	Sì	Sì	Non richiesto	Non richiesto
Per servizi critici: ISO 20000-1:2020	Sì	Sì	Non richiesto	Non richiesto

Per tutti i soggetti sopra elencati, la validità delle relative certificazioni è consultabile sul portale di Accredia.

SUB 2 – CERTIFICAZIONI DEI DATA CENTER IN HOSTING

Le certificazioni possedute da TIM S.p.A. (P.IVA 00488410010) e Noovle S.p.A. (P.IVA 11432040969) possono essere consultate sul registro Accredia, inserendo le partite IVA/Codici fiscali al link https://services.accredia.it/ppsearch/accredia_companymask_remote.jsp?ID_LINK=1739&area=310.
Alla data del presente documento, le certificazioni dei data center superano i requisiti previsti dalla normativa vigente, in particolare per quanto attiene al possesso della certificazione ISO 22237 "Affidabilità Infrastrutture IT".
In aggiunta a quanto richiesto, riguardo agli standard ISO:

a) Il Data center Primario è certificato TIER IV da Uptime Institute (Per riferimento si consulti il link: https://uptimeinstitute.com/tiers), i cui requisiti sono così descritti:
   i. Un data center di livello IV dispone di diversi sistemi indipendenti e fisicamente isolati che fungono da componenti di capacità ridondanti e percorsi di distribuzione. La separazione è necessaria per evitare che un evento comprometta entrambi i sistemi. L'ambiente non sarà influenzato da interruzioni dovute a eventi pianificati e non pianificati. Tuttavia, se i componenti ridondanti o i percorsi di distribuzione vengono chiusi per manutenzione, l'ambiente potrebbe essere esposto a un rischio maggiore di interruzione in caso di guasto.
   ii. Le strutture di livello IV aggiungono tolleranza ai guasti alla topologia di livello III (Un data center di livello III è allo stesso tempo gestibile con componenti ridondanti come elemento chiave di differenziazione, con percorsi di distribuzione ridondanti per servire l'ambiente critico. A differenza del Livello I e del Livello II, queste strutture non richiedono arresti quando le apparecchiature necessitano di manutenzione o sostituzione. I componenti del Livello III vengono aggiunti ai componenti del Livello II in modo che qualsiasi parte possa essere spenta senza influire sul funzionamento dell'I.). Quando un componente dell'apparecchiatura si guasta o si verifica un'interruzione nel percorso di distribuzione, le operazioni IT non verranno influenzate. Per essere compatibili, tutte le apparecchiature IT devono avere un design di alimentazione con tolleranza ai guasti. Anche i data center di livello IV richiedono un raffreddamento continuo per rendere stabile l'ambiente.
b) Entrambi i data centers sono certificati ANSI-TIA 942-B-2017 e in particolare

i. Data Center primario: rated-4 "Fault-Tolerant Site Infrastructure" (Il data center dispone di componenti di capacità ridondanti, percorsi di distribuzione ridondanti attivi per servire le apparecchiature e protezione contro singoli scenari di guasto. Include anche il massimo livello di sicurezza);
ii. Data Center secondario: rated-3 "Concurrently Maintainable Site Infrastructure" (Il data center dispone di componenti di capacità ridondanti e percorsi di distribuzione ridondanti che servono le apparecchiature informatiche, consentendo la manutenzione simultanea di qualsiasi apparecchiatura. Include anche una maggiore sicurezza fisica).

SUB 3 – MISURE DI SICUREZZA DI ALTO LIVELLO

(NOTA: attuazione della Decisione di Esecuzione UE 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra responsabili del trattamento e sub-responsabili del trattamento)

Requisito	Modalità di attuazione
Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico	Esistenza di un processo di *Incident Management*, con Procedura Operativa per la gestione degli incidenti di sicurezza, un Procedura di Gestione dei Sistemi di Backup e di Gestione di Disaster Recovery di replica e ripristino. Strutturazione di più livelli di backup con caratteristiche di segregazione dall'ambiente di produzione e presidi che impediscono la scrittura non autorizzata, su files comunque sottoposti a cifratura.
Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	Periodica effettuazione di Vulnerability Assessment sull'infrastruttura al fine di verificare la presenza di eventuali vulnerabilità e mettere in campo un *remediation plan.*
Misure di identificazione e autorizzazione dell'utente	Presenti soluzioni "*Privileged Access Management*" che consentono l'identificazione, l'autenticazione e processi di autorizzazione con disaccoppiamento dei privilegi amministrativi; Accesso remoto con autenticazione multifattoriale, ammesso esclusivamente da client aziendali autenticati e rispondenti ai requisiti stabiliti dall'organizzazione È effettuata con cadenza mensile una verifica dell'applicazione del processo di gestione degli account ad elevati privilegi. Con frequenza trimestrale vengono rilevate ed analizzate le utenze che non accedono ai sistemi da almeno 180 giorni e vengono implementate le necessarie azioni correttive nell'ambito delle attività assegnate, il personale accede ai dati seguendo le istruzioni che gli sono state impartite utilizzando il proprio account.
Misure di protezione dei dati durante la trasmissione	Il trasferimento dei dati, da e verso il Cliente, è opportunamente protetto. Le situazioni in cui il trasferimento può concretizzarsi sono: Migrazione dei dati del Cliente all'interno dell'Infrastruttura del Cloud Services Provider; Fornitura/Consegna al Cliente di copia dei dati durante il rapporto contrattuale; Restituzione dei dati al Cliente al termine del rapporto contrattuale. In caso di trasferimento telematico dei dati del Cliente, si garantisce l'utilizzo di canali di comunicazione sicuri e cifrati (es: HTTPS, VPN). In caso di trasferimento fisico dei dati del Cliente, devono essere utilizzati esclusivamente supporti fisici contenenti dati preventivamente cifrati. In entrambi i casi il Cliente resta unico sub-responsabile dell'integrità e completezza dei propri dati.
Misure di protezione dei dati durante la conservazione	La strategia di backup adottata, specificata nella relativa Procedura Operativa, prevede l'implementazione e l'utilizzo di soluzioni che consentono una pluralità di repliche in ambienti segregati e segmentati. I dati sono cifrati e sono previste ulteriori misure di sicurezza consistenti nel blocco nativo di scrittura su files; Applicazione di una soluzione di endpoint XDR specifica per analisi comportamentale sotto il controllo del Security Operation Center. I dati sono cifrati a riposo.
Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati	I Data Centers del CSP rispondono ai più alti livelli di sicurezza fisica. Parimenti, le sedi di PA Digitale sono provviste di presidi tecnici antintrusione e sorveglianza h24/7/365

	Esiste una Procedura Operativa per la Gestione della sicurezza fisica e ambientale delle Sedi Aziendali che prevede norme di sicurezza specifiche tra le quali: accesso alle sedi a personale esterno consentito solo previa registrazione in uno specifico Registro Ospiti, presenza di estintori di varie tipologie, gestiti in conformità ai requisiti di legge, la cui collocazione è riportata sulle planimetrie dislocate all'interno dei locali; servizio di vigilanza armata con presidio e ronde; sistemi antintrusione e videosorveglianza e collegamenti con sale operative e forze di polizia;
Misure per garantire la registrazione degli eventi	Il Security Operation Center di gestione autorizza una Soluzione SIEM per la raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete della propria infrastruttura. Il monitoraggio del Security Operation Center è attivo 24/7/365, con procedure di escalation codificate. È attuata la registrazione dei log-in e i log-out degli Amministratori di Sistema ai sensi della normativa vigente.
Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita	Esistono specifiche procedure, documentate in conformità al sistema di gestione adottato, per il controllo dei processi di cambiamento, caratterizzati dalla definizione di requisiti di sicurezza *by design* e *by lifecycle* per il mantenimento della sussistenza dei livelli di sicurezza attesi, riguardo a disponibilità, integrità e riservatezza, coerenti con le risultanze dell'analisi del rischio. La configurazione dei sistemi lato applicativo avviene in base alle indicazioni fornite da PA Digitale, in base alle previsioni contrattuali.
Misure di informatica interna e di gestione e governance della sicurezza informatica	Processo basato sulla gestione del rischio, con revisione annuale degli esiti dell'analisi del rischio e revisione della direzione, in conformità ai processi certificati ISO 27001 (esteso alle ISO 27017 e ISO 27018 associato ai servizio cloud). In applicazione del principio di gestione del rischio, è stato implementato un sistema di ricerca continua di vulnerabilità, con un processo strutturato per priorità nell'applicazione dei rimedi rilasciati dai vendor di prodotto o delle contromisure necessarie.
Misure per garantire la conservazione limitata dei dati	In caso di cessazione del Contratto, anche dovuta a recesso o risoluzione, e/o non rinnovo dello stesso alla scadenza, sono previste specifiche misure contrattuali per consentire ai clienti finali la portabilità dei propri dati (primari e di backup). In alternativa, decorsi 90 (novanta) giorni, si provvede alla cancellazione ed al riutilizzo dello spazio di archiviazione
Modalità per garantire l'assistenza al Titolare	Esiste una disciplina contrattuale che impegna l'intera catena della fornitura a: a. ricevere ed attuare le istruzioni documentate del titolare del trattamento in ogni modalità ed attività di gestione dello stesso, a condizione che le istruzioni ricevute non contrastino con le previsioni normative e regolamentari, in particolare per quanto attiene alla gestione dei requisiti della "Strategia Cloud Italia". È onere del Titolare accertarsi che le istruzioni documentate non duplichino o contrastino con quelle già previste dalla normativa vincolante. In caso di contrasto o duplicazione avranno sempre prevalenza le norme provenienti dalle Pubbliche Autorità; b. consentire al Titolare del trattamento la verifica dei livelli di disponibilità, integrità e riservatezza e l'esame delle misure organizzative e di processo, mediante audit di seconda terza parte e verifiche tecniche di tipo penetration test, previa manleva ed assunzione di piena responsabilità da parte del Titolare; c. garantire la formazione del proprio personale e l'assicurazione dell'impegno alla riservatezza, legalmente vincolante; d. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt.. Da 32 a 36 del GDPR ed in particolare: i. esiste una procedura documentata per la segnalazione degli incidenti di sicurezza e la comunicazione al Titolare degli elementi idonei alla valutazione sulla necessità di notifica all'Autorità di controllo; ii. esiste una procedura di gestione dell'emergenza e della crisi,

	che determina il processo di comunicazione agli interessati, anche mediante comunicazioni pubbliche.
Definizione del perimetro della responsabilità condivisa nei servizi cloud	Una procedura documentata e depositata presso l'Autorità di vigilanza definisce il perimetro di responsabilità nell'erogazione dei servizi in cloud tra il soggetto titolare dell'infrastruttura IaaS ed il fornitore di software in cloud SaaS.

SUB 4 – MISURE DI SICUREZZA DI DETTAGLIO

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
Misure sicurezza Data Center	Accesso al Sistema o SW (autenticazione)	Adozione di misure dirette a garantire che: - gli accessi di amministrazione da parte della SWH siano riservati al personale a cui sia attribuita la qualifica ("ruolo") di amministratore di sistema, in virtù di elevate capacità tecniche e caratteristiche di comprovata affidabilità e moralità; - l'accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA).	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18, 8.15 MM AgID ABSC 5.1.1, 5.4.1, 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.2 - 7.4
Misure sicurezza Data Center	Accesso al Sistema o SW (policy di gestione)	Per i servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali, devono essere previste le seguenti policy: - utenze che consentono l'individuazione dell'amministratore che esegue l'intervento; - attivazione di un processo di log management che identifichi i log in, log out e log in failed; - conservazione dei log in un formato che ne garantisca l'integrità e la lettura nel tempo; - conservazione dei log per almeno sei (6) mesi; - verifica annuale dell'operato degli amministratori di sistema; - accesso ai sistemi attraverso VPN e MFA.	ISO/IEC 27002:2022 5.3 ETSI EN 319 401 clauses 7.2 - 7.4

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
Misure sicurezza Data Center	Log Management	Funzionalità per il tracciamento o registrazione (log) degli accessi e delle attività svolte dagli Utenti. I log concernenti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore di sistema del Cliente o della Software House su richiesta del Cliente.	ISO/IEC 27002:2022 8.15 ETSI EN 319 401 clauses 7.2, 7.4, 7.9, 7.10
Misure sicurezza Data Center	Auditing	Utilizzo del sistema di gestione e analisi dei log anche per il monitoraggio delle attività degli amministratori di sistema. L'accesso al sistema di gestione dei log è riservato al personale avente ruolo di auditor e non è ammesso per il personale addetto all'amministrazione di sistema.	ISO/IEC 27002:2022 8.16 ETSI EN 319 401 clauses 7.2, 7.4, 7.9, 7.10
Misure sicurezza Data Center	Crittografia dei protocolli di comunicazione	Applicazione di protocolli crittografici standard di comunicazione sicuri e non obsoleti, nei casi in cui l'accesso al sistema sia effettuato tramite Internet.	ISO/IEC 27002:2022 5.14, 8.21 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.5, 7.8
Misure sicurezza Data Center	Minacce e Vulnerabilità	Adozione di un programma di gestione delle minacce e dei rischi per monitorare continuamente le vulnerabilità delle Piattaforme SaaS indicate da best practice internazionali attraverso la pianificazione e l'esecuzione di scansioni delle vulnerabilità interne ed esterne e test di penetrazione. Le vulnerabilità identificate devono essere valutate per determinare i rischi associati e le opportune azioni correttive stabilite in base alla priorità assegnata e gravità rilevata.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 5, 7.2, 7.3, 7.6, 7.8
Misure sicurezza Data Center	Firewalling	Adozione di sistemi di firewall finalizzati a filtrare e contenere il traffico identificando eventuale traffico anomalo indicatore di possibili attacchi informatici. Presenza di firewall L4 o L7/WAF.	ISO/IEC 27002:2022 5.14, 8.22 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clause 7.8
Misure sicurezza Data Center	Intrusion Prevention	Protezione dell'ambiente mediante cui è erogato il servizio dalla SWH mediante Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di	ISO/IEC 27002:2022 7.4, 8.21 ISO/IEC 29100:2011 5.11

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
		rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.	ETSI EN 319 401 clauses 7.8, 7.9
Misure sicurezza Data Center	Malware protection	Adozione di misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispamming, antiphishing, etc., mantenuti costantemente aggiornati).	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.7, 7.8, 7.9
Misure sicurezza Data Center	Filesystem Antivirus	Adozione di moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi, con possibilità di configurare, su base progettuale, prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.7, 7.8, 7.9
Misure sicurezza Data Center	Monitoraggio e gestione incidenti	Adozione di policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza.	ISO/IEC 27002:2022 5.24, 5.25, 5.26, 5.27, 5.28, 6.8 ETSI EN 319 401 clause 7.9
Misure sicurezza Data Center	Security Patch Management	Sottoposizione della piattaforma ad un processo periodico di verifica delle patch o delle fix disponibili relativamente alle componenti dell'impianto di erogazione e a quelle ritenute critiche per l'erogazione del servizio o per la sicurezza.	ISO/IEC 27002:2022 8.8 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clause 7.7
Misure sicurezza Data Center	Sicurezza fisica	Applicazione di adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting providers/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.6, 7.8, 7.9
Misure sicurezza Data Center	Anti allagamento	Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
			ETSI EN 319 401 clause 7.6
Misure sicurezza Data Center	Anti intrusione	Impostazione nel Data Center di un sistema di controllo degli accessi che identifichi coloro che accedono e impedisca l'accesso ai non autorizzati. La procedura deve prevedere anche la gestione del Change con l'attivazione e disattivazione dell'autorizzazione all'accesso in funzione dei cambi di ruolo.	ISO/IEC 27002:2022 7.1, 7.2 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.6
Misure sicurezza Data Center	Telecamere a circuito chiuso	Installazione di telecamere (CCTV) per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.	ISO/IEC 27002:2022 7.4 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.6
Misure sicurezza Data Center	Condizionamento	Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati.	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.6
Misure sicurezza Data Center	Continuità ed emergenza	Adozione di procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema/SW (in caso di incidente / violazione di dati personali). Le procedure devono comprendere le indicazioni per la conservazione delle copie di backup nonché un piano per la garanzia di efficace continuità dei servizi erogati.	ISO/IEC 27002:2022 5.4, 5.29 MM AgID ABSC 10 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.1.1, 7.10, 7.11,
Misure sicurezza Data Center	Cancellazione dei dati	Previsione di misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente.	ISO/IEC 27002:2022 8.10 ETSI EN 319 401 clause 7.12
Misure sicurezza Data center esterni	Verifica dei requisiti del sub-fornitore e contrattualizzazione degli obblighi relativi alle misure di sicurezza	Selezione e verifica dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza (previsti dalla SWH per la gestione del DC).	ISO/IEC 27002:2022 5.19; 5.20 ETSI EN 319 401 clauses 6.3, 7.1.1. 7.1.2, 7.2, 7.6, 7.8

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
Misure sicurezza Data center esterni	Audit nei confronti del sub-fornitore	Sottoposizione del sub-fornitore che gestisce il DC esterno ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza, fatto salvo quanto previsto dalle condizioni di servizio fissate da providers multinazionali di servizi di DC ai sensi dell'art. 7.7 del CoC.	ISO/IEC 27002:2022 5.22 ETSI EN 319 401 clauses 6.3, 7.1.1. 7.1.2, 7.2, 7.6, 7.8,
Connettività	Linee Internet e disponibilità di banda	Previsione di misure volte ad assicurare una connettività adeguata in conformità ai livelli di servizio contrattualmente definiti con il Cliente.	ISO/IEC 27002:2022 8.6, 8.21 ETSI EN 319 401 clauses 7.1.1 7.8
Connettività	Firewalling	Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling (riferito alla componente di Software house, per i sistemi IDC vedasi dichiarazione "Misure di sicurezza Data Center/Firewalling).	ISO/IEC 27002:2022 5.14, 8.22, 8.21, 8.23 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clause 7.8
Sicurezza rete	AntiDDoS	Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi ("**DDoS**").	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clause 7.7
Sicurezza rete	IDS/IPS	Adozione di un sistema IPS (Intrusion Prevention System) in grado di bloccare automaticamente gli attacchi rilevati e IDS (Intrusion Detection System) in grado di intercettare le minacce fornendo così una protezione real-time ai servizi erogati dal Data Center.	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11 ETSI EN 319 401 clauses 7.8, 7.9
Governance	Formazione	Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento.	ISO/IEC 27002:2022 6.3 ETSI EN 319 401 clauses 7.1.1, 7.2
Governance	Ubicazione geografica	Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati.	ISO/IEC 27002:2022 5.31 ETSI EN 319 401 clauses 7.1.1, 7.3
Governance	Data Breach	Adozione di procedure di individuazione, contenimento e risoluzione di situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27 ETSI EN 319 401 clauses 7.1.1, 7.8, 7.9

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti
Requisiti sistemistici e di gestione	Sicurezza logica	Rivalutazione con cadenza almeno annuale delle misure e procedure di sicurezza applicate in modo da aggiornarle in relazione alle vulnerabilità rilevate, agli attacchi subiti e all'evoluzione della tecnologia.	ISO/IEC 27002:2022 8.27 MM AgID ABSC 3.1.2 ETSI EN 319 401 clauses 5, 6, 7.1, 7.2, 7.3, 7.6, 7.8,

SUB 5 – MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE ATTUATE DA PA DIGITALE E PRESCRITTE AL CLOUD SERVICES PROVIDER DELL'INFRASTRUTTURA CLOUD, DERIVANTI DALLA NORMATIVA VIGENTE (DETERMINAZIONE ACN 307/2022)

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

In riferimento alla Determinazione ACN n. 306 del 18 gennaio 2022 -" Modello per la predisposizione dell'elenco e della classificazione dei dati e dei servizi della pubblica amministrazione" e e alla Determinazione n. 307 del 18 gennaio 2022, "AGGIORNAMENTO DEGLI ULTERIORI LIVELLI MINIMI DI SICUREZZA, CAPACITÀ ELABORATIVA, E AFFIDABILITÀ DELLE INFRASTRUTTURE DIGITALI PER LA PUBBLICA AMMINISTRAZIONE E DELLE ULTERIORI CARATTERISTICHE DI QUALITÀ, SICUREZZA, PERFORMANCE E SCALABILITÀ DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, NONCHÉ REQUISITI DI QUALIFICAZIONE DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE" (articoli 7, 8, 11 del Regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, adottato dall'Agenzia per l'Italia digitale ai sensi dell'articolo 17, comma 6, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109) erinviando al contenuto dell'allegato B2 di tale provvedimento, PA Digitale S.p.A., alla data del presente documento - è qualificata per l'erogazione di servizi "Ordinari". Tuttavia, in vista dell'ampliamento del processo di qualificazione, sono già in essere misure di sicurezza idonee per il trattamento di dati qualificati dalle Amministrazioni come "Critici". In logica di applicazione delle misure massime, i presidi di sicurezza beneficiano dei controlli previsti per i dati a maggior rilievo nella Strategia Cloud Italia e pertanto, PA Digitale richiede al proprio fornitore di servizi IaaS, quale requisito essenziale del contratto di servizio, i controlli che seguono.

Affidabilità della soluzione complessiva

- Alta affidabilità

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

A.AA-2 : Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità
1. Il Centro di elaborazione dati (CED) deve essere dotato di soluzioni hardware e software (apparati di rete e sicurezza, storage, servizi di virtualizzazione, etc.) per la configurazione dei servizi in alta affidabilità. Devono essere inoltre messe a disposizione *capability* e funzionalità a supporto di configurazioni dei servizi in alta affidabilità quali:
   a. Scelta della replica locale dei dati per un servizio storage;
   b. Presenza di servizi di bilanciamento di carico;
   c. Meccanismi di *anti-affinity* per la distribuzione delle istanze computazionali.

- Governance e processi

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

A.GP-2: È garantito il rispetto degli indicatori di servizio obbligatori

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

- Performance e scalabilità

A.PS-1: Sono garantite caratteristiche minime di connettività
1. Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite: *bandwidth* di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.

Sicurezza della componente applicativa

IDENTIFY (ID)

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

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione
1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.

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

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

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
1. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. È nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.
3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sull'infrastruttura.
4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.
5. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.
6. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.
7. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021, e alle attività di verifica e ispezione

- *Governance* (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella

gestione del rischio di cybersecurity.

ID.GV-1: È identificata e resa nota una policy di cybersecurity

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

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

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

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

ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

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

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

1. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate.
2. L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale.
3. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.
4. Esiste un documento aggiornato di valutazione del rischio (*risk assessment*) che comprende almeno:
    - l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento;
    - le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DE.CM-8;

c. i potenziali impatti ritenuti significativi sull'Infrastruttura digitale, opportunamente descritti e valutati;
d. l'identificazione, l'analisi e la ponderazione del rischio

- *Supply Chain Risk Management* (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento

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

1. Esiste un documento aggiornato di dettaglio che descrive i processi di gestione del rischio inerente la catena di approvvigionamento cyber.
2. Tali processi sono validati e approvati da parte dei vertici del soggetto.

PROTECT (PR)

- *Identity Management, Authentication and Access Control* (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate

PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.

3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).
5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.
7. Esiste un documento aggiornato di dettaglio contenente almeno:
    - 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,
    - 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;
    - i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato
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.
3. E' definito un perimetro di sicurezza tra le aree amministrative e le aree di *data storage* e *processing*.

PR.AC-3: L'accesso remoto alle risorse è amministrato
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.
5. Esiste un documento aggiornato di dettaglio contenente almeno:
    - le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate;
    - i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.
2. È definito un piano per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste.
PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)
1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.

- *Awareness and Training* (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti

PR.AT-1: Il personale del soggetto è informato e addestrato
1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personal del soggetto e le modalità di verifica dell'acquisizione dei contenuti.
2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche:
   a. la tutela della confidenzialità di dati in chiaro o cifrati;
   b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro;
   d. la definizione di ruoli e delle responsabilità;
   e. politiche di accesso a sistemi, asset e risorse;
   f. politiche di gestione delle informazioni e della sicurezza;
   g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;
   h. requisiti per la non divulgazione/confidenzialità di informazioni.

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

- *Data Security* (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.

PR.DS-1: I dati memorizzati sono protetti
1. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
2. Con riferimento alle infrastrutture, al trattamento dei dati e dei servizi dell'Amministrazione, resta fermo quanto previsto dall'allegato A al Regolamento, requisito IN-SA-PR.DS-1-01.
3. Con riferimento all'accesso ai dati da parte di entità extra-UE, il soggetto:
   a. segnala all'Agenzia per la Cybersicurezza Nazionale (ACN) e all'Amministrazione ogni richiesta di accesso a dati o metadati da parte di entità extra-UE;
   b. fornisce accesso a dati dell'Amministrazione o metadati ad entità extra-UE solo a valle di un'autorizzazione esplicita da parte dell'Amministrazione.

PR.DS-2: I dati sono protetti durante la trasmissione
1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.

PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
1. Sono definite in relazione alla categoria ID.AM, almeno:
   a. le politiche di sicurezza adottate per il trasferimento fisico, la rimozione e la distruzione di dispositivi atti alla memorizzazione di dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
1. Sono definite in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per l'accesso ai dati;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Sono adottate politiche di *Data Loss Prevention* coerentemente con la valutazione dei rischi.

PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
1. Sono definite in relazione alla categoria ID.AM, almeno:
   a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni;
   b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
1. Sono definite in relazione alla categoria ID.AM, almeno:
   a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata;

b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione;
c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

- *Information Protection Processes and Procedures* (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale

PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni
1. Sono definite:
   a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. È implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione
3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. rollback) in caso di errori o problemi di sicurezza.

PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati
1. 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"
3. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
   - le politiche di sicurezza adottate per il *backup* delle informazioni;
   - i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
1. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi l'Infrastruttura digitale.
2. Esiste un documento aggiornato di dettaglio contenente i piani di continuità operativa, nonché quelli di risposta in caso di incidenti, che comprende almeno:
   a. le politiche e i processi impiegati per identificare le priorità degli eventi;
   b. le fasi di attuazione dei piani;
   c. i ruoli e le responsabilità del personale;
   d. i flussi di comunicazione e reportistica;
   e. il raccordo con il CSIRT Italia.
3. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
4. I piani di *business continuity* sono collaudati e comunicati alle parti interessate.
5. La documentazione di cui al punto 2 è resa disponibile all'Amministrazione e rivista periodicamente.
6. L'impatto derivante da interruzioni ed eventuali rischi è determinato al fine di stabilire i criteri per sviluppare strategie e capacità di business continuity.

PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità
1. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. le politiche di sicurezza adottate per gestire le vulnerabilità;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, delle *threat signatures* e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale.

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

PR.MA-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati
1. Sono definite in relazione alla categoria ID.AM:
   a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

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

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.

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

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

- *Protective Technology* (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. Sono definite:
   a. le politiche di sicurezza adottate per la gestione dei log dei sistemi;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.

PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse

1. In relazione ai piani previsti dalla sottocategoria PR.IP-9:
   a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;
2. Esistono meccanismi per garantire la continuità operativa, nel rispetto delle misure di sicurezza qui elencate.
3. Sono definite:
   a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DETECT (DE)

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

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

1. Ai fini di rilevare tempestivamente incidenti con impatto dell'infrastruttura, sono adottati gli strumenti tecnici e procedurali per:
   a. acquisire le informazioni da più sensori e sorgenti;
   b. ricevere e raccogliere informazioni inerenti alla sicurezza dell'infrastruttura rese note dal CSIRT Italia, da fonti interne o esterne al soggetto;
   c. analizzare e correlare, anche in maniera automatizzata, i dati e le informazioni di cui alle lettere a), b) e c), per rilevare tempestivamente eventi di interesse.
2. Le attività di analisi e correlazione di cui al punto precedente sono monitorate e registrate. La relativa documentazione, anche elettronica, è conservata per almeno 24 mesi.
3. Sono definite:
   a. le politiche applicate per individuare i sensori e le sorgenti di cui al punto 1, lettera a);
   b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al punto 1, lettere a) e b);
   c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al punto 1, lettera c).
   d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al punto 2.
4. Sono presenti politiche e procedure di *logging*, monitoraggio, sicurezza e conservazione di registri di accesso, le quali dovranno essere aggiornate almeno su base annuale.
5. È adottato un sistema di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati.
6. Sono definiti e valutati processi, procedure e misure tecniche per la segnalazione di anomalie e guasti del sistema di monitoraggio e in grado di fornire una notifica immediata al soggetto responsabile.

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

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

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

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

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

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

DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability
1. Le nomine di cui alla sottocategoria ID-AM-6 sono rese note all'interno del soggetto.
2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
   a. i ruoli, i processi e le responsabilità di cui al punto 2;
   b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.
4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate.

RESPOND (RS)

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

RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
1. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.
2. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.

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

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

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

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

RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)
1. Sono definiti e mantenuti contatti con gruppi di interesse legati all'infrastruttura digitale e altre entità rilevanti e in linea con il contesto del soggetto in relazione all'infrastruttura digitale.
2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.

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

RS.An-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)
1. Gli esiti delle valutazioni di cui alla sottocategoria DE.AE-3 e dei *penetration test* e *vulnerability assessment* di cui alla sottocategoria DE.CM-8, qualora disponibili, sono diffusi alle articolazioni competenti del soggetto.
2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati.
3. Esiste un documento aggiornato che descrive, almeno:
   a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2;
   b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.

RECOVER (RC)

- *Recovery Planning* (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.

RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
1. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.
2. Il piano di ripristino viene testato, su base semestrale, nell'ambito di due esercitazioni annuali.

Data Center Security - misure di sicurezza fisica e infrastrutturale

S.DC-01: I Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale
1. Il soggetto garantisce il presidio operativo del Data Center 24/7/365.
2. Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA- 942, EN 50600, Uptime Institute Tier Certification o analoghi.
3. Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.
4. Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.
5. Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).

S.DC-02: Sono adottate misure di sicurezza fisica e ambientale
1. Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste

policy e procedure dovranno essere riviste su base almeno annuale.
2. Sono implementati, manutenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato.
3. Sono implementati, mantenuti e adottati, all'interno dei Data Center, i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.

Datacenter Security – criteri di progettazione ai fini della manutenzione

A.DC-1: La progettazione/realizzazione del Data Center garantisce la manutenibilità a caldo, conformemente agli standard di mercato.
1. L'infrastruttura digitale deve aderire ai parametri del certificato ANSI/TIA 942B con rating "*Concurrent Maintainability*" oppure a quello di Tier III dell'Uptime Institute. In alternativa deve essere conforme alle caratteristiche costruttive, degli impianti meccanici, elettrici e antincendio riportati alla Tabella 2.

Capacità elaborativa

CE.CE-01: Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore
1. La capacità elaborativa dell'Infrastruttura Digitale è gestita attraverso un processo formale aderente alle *best practice* sul *capacity management* ITIL o alle linee guida presenti alla ISO/IEC 20000-2.

Risparmio energetico

RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore
1. Il soggetto ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti dai suoi Data Center (es. ISO 14064), o per la gestione dell'energia dei propri Data Center (es. ISO 50001), o per la gestione ambientale dei propri Data Center (es. ISO 14001).

RE-GE-02: Valutazione annuale dell'efficienza energetica del Data Center
2. 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.

Affidabilità dell'infrastruttura digitale sottostante

- Alta affidabilità

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

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

- Governance e processi

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

A.GP-2: È garantito il rispetto degli indicatori di servizio obbligatori
3. 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.
4. 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.

- Performance e scalabilità

A.PS-1: Sono garantite caratteristiche minime di connettività
1. Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite: *bandwidth* di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.

- Business Continuity e Disaster Recovery

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

Tabella 1-Indicatori minimi di servizio dell'Infrastruttura

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

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

Best practices ANsI/TIA942, Normativa Anti-incendio nazionale

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

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

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

Controllo dell'umidità nella Computer Room	All'interno della *Computer Room* è monitorata l'umidità dell'aria.
Unità interne sistemi di raffreddamento ad acqua	Le unità interne dei sistemi raffreddati ad acqua sono ridondate (ogni 5-8 unità installate deve essere presente un'unità aggiuntiva).
Alimentazione elettrica agli apparati meccanici	L'alimentazione elettrica dei sistemi è ridondata (N+1) e configurata per garantire la manutenzione a caldo.
Sistema di controllo HV AC	Il sistema di controllo della ventilazione e del condizionamento dell'aria è progettato per garantire la manutenzione a caldo.
Sistemi condensati ad acqua, Ripristino livello acqua dei circuiti	Per i sistemi condensati ad acqua, il ripristino del livello di acqua nei circuiti deve avere due punti di connessione alla rete di alimentazione dell'acqua.
Quantità di carburante per i generatori	La quantità di carburante per i generatori garantisce un'autonomia di 48 ore (previo possesso di permesso specifico rilasciato dai Vigili del Fuoco).
Serbatoi per Carburante per i generatori	Sono presenti serbatoi multipli per il carburante per i generatori.
Pompaggio carburante e tubazioni per i generatori	Per ogni generatore è previsto il pompaggio del carburante e le tubazioni per i generatori.
Impianto antincendio	È presente un impianto Sprinkler per rilevazione e spegnimento dell'incendio nella parte uffici dell'edificio, o secondo le prescrizioni dei Vigili del Fuoco.
Rilevazione Fumi VESDA per *Computer Room* ed *Entrance Room* con presenza di apparati attivi o sistema equivalente	Nelle computer Room e nell'*entrance room* l'impianto antincendio è usata la tecnologia VESDA o un sistema equivalente per la rilevazione dei fumi.
Spegnimento automatico a gas per *Computer Room* ed *Entrance Room*.	Nelle computer Room e nell'*entrance room* è presente un impianto per lo spegnimento automatico a gas, con la presenza di apparati attivi.
Sistema anti-allagamento per *Computer Room* ed *Entrance Room* con presenza di apparati attivi	Nelle *computer Room* e nell'*entrance room* è presente un impianto antiallagamento, con la presenza di apparati attivi.

5.2. Livelli minimi di sicurezza e affidabilità servizio SAAS

Classificazione dati: ordinari-critici

Qualità del servizio (SLA)

QU.SE-1: Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore
1. Il sistema di gestione della qualità del servizio cloud è adottato formalmente dal soggetto in conformità allo standard UNI EN ISO 9001:2015-Sistemi di Gestione per la qualità.
2. Il sistema di gestione dei servizi IT del servizio cloud è adottato formalmente dal soggetto in conformità allo standard ISO/IEC 20000-1 :2018-Sistema di gestione dei servizi IT.

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

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

QU.SE-4: Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud
1. Devono essere rese disponibili all'Amministrazione le linee guida per una gestione sicura del servizio cloud oggetto di qualificazione, indirizzando, ove applicabile, i seguenti aspetti:
a. Istruzioni per una configurazione sicura;
b. Informazione su vulnerabilità note e meccanismi di aggiornamento;
c. Gestione degli errori e meccanismi di *logging;*
d. Meccanismi di autenticazione;
e. Ruoli e diritti, comprese le combinazioni che risultano in un rischio elevato;
f. Servizi e funzioni per l'amministrazione del servizio da parte di utenti privilegiati;
g. Le linee guida vengono fornite e mantenute nelle modalità e tempistiche di cui alla misura IP.GR-01.

Livello del servizio (SLA)

QU.LS-1: E garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative
1. Il soggetto garantisce aderenza agli obiettivi (SLO) corrispondenti agli indicatori di servizio (SLI) riportati in Tabella 1 "Indicatori della qualità del Servizio" e ne garantisce il rispetto nei rapporti contrattuali nella forma di accordi relativi ai livelli di servizio (SLA). Il soggetto può comunicare all'Amministrazione eventuali ulteriori indicatori della medesima tabella, o indicarne di nuovi, che potranno essere inseriti come impegni contrattuali con specifici SLO nei rapporti contrattuali.
2. Il soggetto garantisce che venga definita la modalità di condivisione delle informazioni dei livelli di servizio atteso garantiti (SLA) del servizio cloud con l'Amministrazione (es. report periodico) e che, qualora successivamente all'avvio della fornitura si dovesse rendere necessaria una qualsiasi modifica ai livelli di servizio garantiti, questa dovrà essere preventivamente notificata all'Amministrazione per ottenerne la sua approvazione.
3. Il soggetto garantisce l'applicazione di penali compensative da corrispondere all'Amministrazione in caso di violazione dei livelli di servizio garantiti dal contratto di fornitura del servizio qualificato. I metodi di quantificazione e le condizioni di riconoscimento delle penali compensative sono inclusi nel contratto e sono allineati ai valori e alle condizioni di mercato riscontrabili per servizi analoghi o appartenenti alla medesima categoria.

QU.LS-2: Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione
1. All'interno dei Service Level Agreement (SLA) tra il soggetto e l'Amministrazione sono presenti limitazioni con riferimento a modifiche che abbiano impatto direttamente sugli ambienti e/o *tenant* di proprietà dell'Amministrazione.

QU.LS-3: Esistono contenuti e caratteristiche minimi per i Service Level Agreement
1. Ogni SLA tra il soggetto e l'Amministrazione tiene conto di quanto segue:
a. Ambito, caratteristiche e ubicazione della relazione commerciale e dei servizi offerti;
b. Requisiti di sicurezza delle informazioni (incluso il SSRM - *Shared Security Responsibility Model);*
c. Processo di *Change Management;*
d. *Logging* e *Monitoring;*
e. Gestione degli incidenti e procedure di comunicazione;
f. Diritto di audit e valutazione da parte di terzi;
g. Terminazione del servizio;
h. Requisiti di interoperabilità e portabilità;
i. Riservatezza dei dati.

QU.LS-4: è disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato.
1. Il soggetto rende disponibile all'Amministrazione l'accesso ad uno o più strumenti di monitoraggio per il servizio cloud. Essi devono consentire attività di raccolta, monitoraggio, filtraggio, creazione di report attraverso parametri predefiniti o parametrizzabili e consentire all'Amministrazione di impostare allarmi personalizzati. La granularità massima delle operazioni non deve essere superiore al minuto (ad es., deve essere possibile filtrare o raccogliere gli eventi ogni

minuto). In aggiunta, il soggetto specifica l'eventuale disponibilità di API e strumenti di monitoraggio di terze parti integrate nativamente con il servizio qualificato.

Sicurezza

IDENTIFY (ID)

Asset Management

ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione
1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.
2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete a consentito esclusivamente a quelli approvati.

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

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

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
1. è definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. è nominato, nell'ambito dell'articolazione di cui al punto 1, un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.
3. Sono nominati, nell'ambito dell'articolazione di cui al punto 1, un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sul servizio cloud.
4. L'incaricato di cui al punto 2 e il referente tecnico di cui al punto 3 operano in stretto raccordo.

ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
5. I nominativi e gli estremi di contatto dell'incaricato di cui al punto 2 e del referente tecnico di cui al punto 4 sono comunicati dal soggetto all'Agenzia per la Cybersicurezza Nazionale (ACN).
6. Esiste un elenco contenente tutto il personale interno ed esterno impiegato nei processi di cybersecurity aventi specifici ruoli e responsabilità. L'elenco è disseminato presso le articolazioni competenti del soggetto.
7. Esiste un elenco delle figure analoghe all'incaricato di cui al punto 2 e al referente tecnico di cui al punto 3 presso terze parti, in relazione alle dipendenze esterne, e presso lo stesso soggetto, in relazione alle dipendenze interne. Le competenze dell'incaricato e del referente tecnico devono essere rivalutate in funzione della tipologia di dipendenza. L'elenco è disseminato presso le articolazioni competenti del soggetto.
8. L'incaricato di cui al punto 2 assicura, inoltre, la collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN), anche in relazione alle attività connesse all'articolo 5 del decreto-legge 105/2019 e alle attività di prevenzione,

preparazione e gestione di crisi cibernetiche affidate al Nucleo per la CyberSicurezza (NCS) di cui al decreto-legge 82/2021.

Governance

ID.GV-1: E identificata e resa nota una policy di cybersecurity
1. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.
2. II 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-1: E identificata e resa nota una policy di cybersecurity
3. Ogni scostamento dai livelli minimi di sicurezza definito internamente nel documento di cui al punto 1 deve essere identificato, gestito ed eventualmente autorizzato dal soggetto attraverso un processo di governance strutturato
4. Esiste un documento aggiornato recante indicazioni in merito alla pianificazione, ai ruoli, all'implementazione, operazione, valutazione, e miglioramento di programmi di cybersecurity sia in relazione al personale interno che per eventuali terze parti

ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity
1. Il documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity.
2. Esiste un programma formale di Enterprise Risk Management (ERM) che include politiche e procedure per l'identificazione, la valutazione, la proprietà, il trattamento e l'accettazione dei rischi di sicurezza e privacy del cloud.

Risk Assessment

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

ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate
3. Le relazioni periodiche delle verifiche e dei test di cui al punto 1 devono contenere almeno:
a. la descrizione generale delle tipologie di verifiche effettuate e gli esiti delle stesse;
b. la descrizione dettagliata delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza;
c. il livello di esposizione delle risorse del sistema cui è possibile accedere a seguito dello sfruttamento delle vulnerabilità.
4. Esiste un documento per la correzione delle vulnerabilità che prevede anche, la notifica alle parti interessate.

ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
1. L'analisi del rischio a 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.

ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
4. Esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno:

a. l'identificazione delle minacce, sia interne che esterne, opportunamente descritte e valutate e le relative probabilità di accadimento;
b. le vulnerabilità di cui alla sottocategoria ID.RA-1 e alla sottocategoria DE.CM-8;
c. i potenziali impatti ritenuti significativi sul servizio cloud, opportunamente descritti e valutati;
d. l'identificazione, l'analisi e la ponderazione del rischio

Supply Chain Risk Management

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

ID.SC-1: I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione
3. Sono presenti politiche e procedure per la definizione, implementazione e applicazione del modello di responsabilità della sicurezza condivisa *(Shared Security Responsibility Model-SSRM)* all'interno dell'organizzazione, le quali dovranno essere riviste e aggiornate almeno su base annuale.
4. Il modello SSRM è applicato a tutta la catena di approvvigionamento cyber, ivi inclusi altri servizi cloud utilizzati dall'organizzazione.
5. E fornita una chiara definizione in merito alla condivisione delle responsabilità.

ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber
1. In merito all'affidamento di forniture per i servizi cloud sono adottate misure in materia di sicurezza della catena di approvvigionamento cyber attraverso:
a. il coinvolgimento dell'organizzazione di *cybersecurity,* tra cui l'incaricato di cui alla sottocategoria ID.AM-6, punto 2, nel processo di fornitura, già a partire dalla face di progettazione;
b. fatti salvi documentati limiti tecnici, il rispetto del requisito di fungibilità, con la possibilità di ricorrere alla scadenza ad altro fornitore;
c. fatti salvi documentati limiti tecnici, la diversificazione dei fornitori e la conseguente resilienza del servizio cloud;
d. la valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno:
i. della qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria catena di approvvigionamento e la priorità data agli aspetti di sicurezza;
ii. della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.
2. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari per la fornitura di servizi cloud, nonché di dipendenze esterne, corredato dalla relativa documentazione del processo di valutazione di cui al punto 1.

ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber.
1. Le misure di sicurezza implementate dal soggetto in relazione a dipendenze interne sono coerenti, anche in relazione agli esiti dell'analisi del rischio, con le misure di sicurezza applicate al servizio cloud. A tal fine, i contratti, gli accordi o le convenzioni sono aggiornati di conseguenza.

ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali
1. Esiste un documento aggiornato che descrive il processo, le modalità, la cadenza delle valutazioni per i fornitori e partner terzi, proporzionate agli esiti dell'analisi del rischio effettuata.
2. Esiste una pianificazione aggiornata degli audit, delle verifiche o di altre forme di valutazione previste, nonché un registro di quelli effettuati e la relativa documentazione.

3. è definito ed implementato un processo di *Audit Management* al fine di consentire lo svolgimento di valutazioni indipendenti e di garanzia, nel rispetto dei principali standard di settore, almeno su base annuale e secondo una pianificazione che tenga conto del rischio
4. Le politiche e procedure di audit e garanzia degli standard, devono essere stabilite, documentate, approvate, mantenute e riviste almeno annualmente.
5. E definito, documentato, approvato, comunicato, applicato e mantenuto un piano di *Remediation.*

PROTECT (PR)

Identity Management, Authentication and Access Control

PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza
1. Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
2. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1, le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.
3. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.
4. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es., trasferimento di personale).
5. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.
6. Esiste una pianificazione aggiornata degli audit di sicurezza delle identità digitali previsti e un registro degli audit effettuati con la relativa documentazione.

PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza
7. Esiste un documento aggiornato di dettaglio contenente almeno:
a. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e le procedure di cui ai punti 1, 2, 3, 4, 5, 6;
b. le politiche di sicurezza adottate per l'amministrazione, la verifica, la revoca e l'audit di sicurezza delle identità digitali e delle credenziali di accesso per gli utenti;
c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.AC-3: L'accesso remoto alle risorse è amministrato
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. E 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-3: L'accesso remoto alle risorse è amministrato
5. Esiste un documento aggiornato di dettaglio contenente almeno:
a. le politiche di sicurezza adottate per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.AC-4: 1 diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
1. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno:

a. le risorse censite a cui è necessario accedere, con riferimento alla categoria ID.AM, per quali funzioni e con quali autorizzazioni;
b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni;
c. l'assegnazione degli utenti censiti a gruppi di utenti.
2. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.
3. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.

PR.AC-4: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni
4. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.
PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)
1. Sono presenti politiche e procedure per la sicurezza dell'infrastruttura di rete, le quali dovranno essere aggiornate almeno su base annuale.
2. E presente una pianificazione per il monitoraggio della disponibilità, qualità e l'adeguata capacità delle risorse al fine di fornire le prestazioni di sistema richieste

PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)
1. Sono definite e implementate politiche e procedure per l'accesso ai sistemi, alle applicazioni e ai dati, compresa l'autenticazione multifattoriale almeno per gli utenti privilegiati e l'accesso a dati.
2. In relazione al servizio cloud, deve essere garantita all'Amministrazione la funzionalità di autenticazione a più fattori o l'uso di soluzioni di autenticazione a più fattori di terze parti. Devono essere rese disponibili informazioni trasparenti in merito alle funzionalità di autenticazione a pia 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).

Awareness and Training

PR.AT-1: Il personale del soggetto e informato e addestrato
1. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti.
2. L'addestramento e la formazione di cui al punto 1 fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche:
a. la tutela della confidenzialità di dati in chiaro o cifrati.
b. la restituzione dei Beni di natura aziendale al termine del rapporto di lavoro
d. la definizione di ruoli e delle responsabilità
e. politiche di accesso a sistemi, asset e risorse
f. politiche di gestione delle informazioni e della sicurezza
g. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi
h. requisiti per la non divulgazione/confidenzialità di informazioni

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

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

Data Security

PR.DS-1: 1 dati memorizzati sono protetti

1.Sono definite, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud al trattamento dei dati e dei servizi dell'Amministrazione, fermo restando quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01, qualora sussistano motivate e documentate limitazioni di carattere tecnico, eventuali metadati necessari per l'erogazione del servizio cloud possono essere trattati mediante l'impiego di infrastrutture fisiche e tecnologiche localizzate al di fuori del territorio dell'Unione europea. In tal caso, i citati metadati non possono contenere, anche in parte, i dati dell'Amministrazione.
3. Con riferimento all'accesso ai dati da parte di entità extra-UE, it 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. E 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. E 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. E 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 a 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-1: I dati memorizzati sono protetti

7. Nel caso di dati e di servizi critici delle Amministrazioni, non trovano applicazione le previsioni del requisito di cui alla sezione 2.2.7, PR.DS-1, punto 2. Con riferimento alle infrastrutture impiegate per l'erogazione del servizio cloud, nonché al trattamento dei dati e dei servizi dell'Amministrazione, ivi inclusi i metadati, resta fermo, pertanto, quanto previsto dall'allegato B al Regolamento, requisito SC-SI-PR.DS-1-01.
8. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza
9. Il servizio cloud supporta un meccanismo di cifratura di tipo *Bring Your Own Key* (BYOK), che consente all'Amministrazione di generare autonomamente, almeno la chiave principale di cifratura (root key), attraverso un HSM ospitato, alternativamente, presso:
a. propria infrastruttura
b. infrastruttura messa a disposizione dal fornitore all'Amministrazione in modalità dedicata
c. infrastruttura di una terza parte scelta dall'Amministrazione.
10. Il soggetto mette a disposizione la funzionalità di importazione sicura delle chiavi di cui al punto 10 nel cloud, per l'esercizio di tutte le operazioni di gestione delle chiavi e della cifratura nel cloud.
11. Sono definite ed implementate procedure e misure tecniche misure per la distruzione delle chiavi memorizzate al di fuori di un ambiente sicuro e revocare le chiavi memorizzate nei moduli di sicurezza hardware (HSM) quando non sono pia 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-2: I dati sono protetti durante la trasmissione
1. Sono utilizzati canali di comunicazione sicuri e criptati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud. Tali canali devono includere solo protocolli aggiornati e approvati.

PR.DS-3:11 trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formate
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-3: II trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale
2. Sono abilitate capacità di geo-localizzazione remota per tutti i dispositivi mobili gestiti [SaaS]
3. Sono definite ed implementate adeguate tecniche di cancellazione dei dati dell'Amministrazione da remoto [SaaS]

PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)
1. Sono definite in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per l'accesso ai dati;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Sono adottate politiche di *Data Loss Prevention* coerentemente con la valutazione dei rischi.

PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
1. Sono definiti in relazione alla categoria ID.AM, almeno:
a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni;
b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi a applicato a quale risorsa;
c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza

PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
1. Sono definite in relazione alla categoria ID.AM:
a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione 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.

Information Protection Processes and Procedures

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
1. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale. [IaaS, SaaS]

PR.IP-1: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)
2. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e il dispiegamento delle sole configurazioni adottate;

b. l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento;
c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza. [SaaS]
3. Sono definiti e documentati requisiti di base per la sicurezza delle diverse applicazioni
4. Sono definite ed implementate metriche tecniche e operative in linea con i requisiti di sicurezza e gli obblighi di conformità
5. Esiste un processo di mitigazione e ripristino per la sicurezza delle applicazioni, automatizzando la mitigazione automatizzata delle vulnerabilità quando possibile.
6. E presente un processo per la convalida della compatibilità del dispositivo con sistemi operativi e applicazioni [PaaS, SaaS]
7. E presente un sistema di gestione delle variazioni in termini di sistema operativo, patching e/o applicazioni [PaaS, SaaS].

PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
1. Sono implementate linee guida e misure tecniche/organizzative per lo sviluppo sicuro del servizio cloud, in aderenza alle linee guida OWASP in merito alla sicurezza nello sviluppo del software (requisiti, progettazione, implementazione, test e verifica). Devono essere resi disponibili all'Agenzia per la Cybersicurezza Nazionale (ACN) e alla Amministrazione i report sui test OWASP condotti, garantendo l'assenza di vulnerability di tipo "high" o "critical".

PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni
1. Sono definite:
a. le politiche di sicurezza adottate per L'aggiornamento delle configurazioni dei sistemi IT e di controllo industriale e per il controllo della modifica delle configurazioni in use rispetto a quelle previste;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. E implementata una procedura per la gestione delle eccezioni, incluse emergenze, nel processo di modifica e configurazione.
3. Sono definiti e implementati piani di ripristino allo stato precedente (cd. *rollback)* in caso di errori o problemi di sicurezza.

PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati
1. Sono definite, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per il *backup* delle informazioni;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Viene effettuato periodicamente un *backup* dei dati memorizzati nel cloud. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup
3. Le copie di backup di informazioni, software e immagini di sistema del servizio cloud sono protette con crittografia forte ed archiviate regolarmente in siti remoti (nel rispetto di quanto previsto dalla categoria PR.DS). Qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta con crittografia forte.
4. Viene verificato periodicamente il ripristino (test di *restore)* delle copie di backup come da obiettivo (SLO) identificato per il corrispondente indicatore di servizio (SLI) riportato alla Tabella 1 "Indicatori minimi della qualità del Servizio"

PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati
5. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per il *backup* delle informazioni;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
6. Esiste un documento aggiornato di dettaglio recante i processi di cui al punto 1.

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
1. L'impatto derivante da interruzioni di business ed eventuali rischi a 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 e resa disponibile, ove richiesto, all'Amministrazione e rivista periodicamente.

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
6. Esiste un documento aggiornato di dettaglio che indica i livelli di servizio attesi dal servizio cloud e, se previsti, dalle hot-replica e/o cold-replica nonché dal sito(i) di *disaster recovery,*
7. Esiste un documento aggiornato di dettaglio contenente i piani di *disaster recovery,* nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno:
a. le politiche e i processi impiegati per identificare le priorità degli eventi;
b. le fasi di attuazione dei piani;
c. i ruoli e le responsabilità del personale;
d. i flussi di comunicazione e reportistica;
e. il raccordo con il CSIRT Italia
8. Esiste un documento aggiornato recante l'elenco delle attività di istruzione, formazione ed esercitazione svolte.
9. Le strategie di *disaster recovery* sono collaudate e comunicate alle parti interessate.
10. I dispositivi critici per il funzionamento del servizio cloud sono ridondati e, se situati in località diverse, ad una distanza in linea con le migliori pratiche del settore

PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerability
1. Esiste un documento aggiornato di dettaglio che indica almeno:
a. le politiche di sicurezza adottate per gestire le vulnerability;
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-12: Viene sviluppato e implementato un piano di gestione delle vulnerability
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.

Maintenance

PR.MA-1: La manutenzione e la riparazione delle risorse e dei sistemi e eseguita e registrata con strumenti controllati ed autorizzati
1. Sono definite anche in relazione alla categoria ID.AM, almeno:
a. le politiche di sicurezza adottate per la registrazione della manutenzione e riparazione delle risorse e dei sistemi;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
1. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PRAC-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.

PR.PT-1; Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
1. I log sono conservati in modo sicuro, possibilmente centralizzato, per almeno 24 mesi.
2. Sono definite:
a. le politiche di sicurezza adottate per la gestione dei log dei sistemi;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza con particolare riguardo all'integrità e alla disponibilità dei log.

PRPT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse
1. In relazione ai piani previsti dalla sottocategoria PRIP-9:
a. sono adottate architetture ridondate di rete, di connettività, nonché applicative;
2. Esistono meccanismi per garantire la continuità di servizio, nel rispetto delle misure di sicurezza qui elencate.
3. Sono definite:
a. le politiche di sicurezza adottate in relazione ai punti 1 e 2;
b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

DETECT

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

8. Per il servizio oggetto di qualificazione deve essere garantita la possibilità di integrare i log nel sistema SIEM di gestione e monitoraggio dell'Amministrazione e che i file di log siano facilmente esportabili dall'Amministrazione, preferibilmente tramite APL

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

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

DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability
1. Le nomine di cui alla sottocategoria ID.AM-6 sono rese note all'interno del soggetto.
2. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud sono ben definiti e resi noti alle articolazioni competenti del soggetto.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
a. i ruoli, i processi e le responsabilità di cui al punto 2;
b. i processi per la diffusione delle nomine, dei ruoli e dei processi di cui ai punti 1 e 2.
4. È definito ed implementato un sistema per la notifica all'Amministrazione degli eventi anomali che coinvolgono le applicazioni e l'infrastruttura sottostante, identificati sulla base di metriche previamente concordate [PaaS, SaaS].

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

RS.C0-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente
1. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di cui al punto 1 sono ben definiti e resi noti alle articolazioni competenti del soggetto.
2. Sono eseguite periodicamente esercitazioni.
3. Esiste un documento aggiornato di dettaglio che indica almeno:
a. le fasi, i processi, i ruoli e le responsabilità di cui ai punti 1 e 2;
b. i processi per la diffusione delle fasi, dei processi, dei ruoli e delle responsabilità di cui ai punti 1 e 2;
c. le modalità per le esercitazioni di cui al punto 3.

RS.C0-5; E attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)
1. Sono definiti e mantenuti contatti con gruppi di interesse legati al cloud e altre entità rilevanti e in linea con il contesto del soggetto.
2. Sono definiti e mantenuti punti di contatto con le autorità di regolamentazione applicabili, le forze dell'ordine nazionali e locali e altre autorità giurisdizionali legali.

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

2. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati.
3. Esiste un documento aggiornato che descrive, almeno:
a. le modalità per ricevere, analizzare e rispondere almeno alle informazioni raccolte tramite le attività di cui ai punti 1 e 2;
b. i processi, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui ai punti 1 e 2.

SUB 6 – LIVELLI DI SERVIZIO

ID SLI	SERVICE INDICATOR LEVEL (SLI)	DESCRIZIONE	MINIMUM SERVICE LEVEL OBJECTIVE (SLO)
SL1	Disponibilità	La percentuale di tempo in un anno in cui l'infrastruttura risulta essere accessibile e usabile	99,8% al netto dei fermi programmati (ovvero pari a 17h, 31m, 53s in un anno solare 99,6% comprendendo i fermi programmati (ovvero pari a 1 giorno 11h, 3m, 47s in un anno solare)
SL2	Attività di supporto (Support hours)	L'orario in cui il servizio di supporto tecnico è operativo per emergenze.	24x7
SL3	Attività di supporto (Support hours) **minime**	L'orario minimo in cui il servizio di supporto tecnico è operativo	Business hours: lunedì-venerdì, dalle 8 alle 18
SL4	Attività di supporto - First Support Response Time	Il tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta iniziale alla segnalazione da parte del soggetto	1h
SL5	Recovery Time	Il tempo massimo necessario a ripristinare completamente il servizio dopo un'interruzione dovuta ad un "evento catastrofico" che ha innescato l'attivazione di un ambiente di erogazione secondario (disaster recovery[5]).	4h
SL6	Recovery Point	L'intervallo massimo di tempo che precede un "evento catastrofico" rispetto al quale si può verificare la perdita delle modifiche ai dati come conseguenza delle attività di ripristino del servizio (disaster recovery[6]).	4h
SL7	Backup testing	Il numero minimo di test di restore (a partire dai dati di backup) eseguiti in un anno)	1
SL8	Comunicazione	L'intervallo di tempo massimo per notificare l'Amministrazione di un incidente o data breach, a valle della registrazione della segnalazione e classificazione dell'evento	1h dalla registrazione dell'evento

[5] PA Digitale adotta logiche di Business Continuity rispetto ai Data center superiori ai livelli richiesti da processi di Disaster Recovery, riducendo i tempi di latenza tra i data Center

FINE DOCUMENTO