

Norme di Sicurezza e Adeguamento

Pieve Fissiraga, 15/05/2025

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**

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

Indice

1. Inquadramento.....	4
1.1. Urbi Smart: Cloud Computing e licenza d'uso.....	4
1.2. WebTec: Cloud Computing	5
1.3. Servizio di Conservazione Digitale a Norma CDAN.....	5
1.4. Cloud: vantaggi	6
2. Le Certificazioni di PA Digitale.....	6
3. Ottemperanza al Regolamento UE 2016 / 679 (GDPR) e relative misure di sicurezza (art. 32).....	7
4. Sicurezza dei dati, continuità operativa, verifiche di conformità attraverso audit e test.	8
4.1. Sicurezza ed affidabilità della rete dati	9
4.2. Infrastruttura di sistema.....	9
4.3. Sottosistema di virtualizzazione.....	10
4.4. Sottosistema storage.....	10
4.5. Sottosistemi firewall e componenti di sicurezza.....	10
4.6. Politiche di backup.....	10
5. La gestione della sicurezza e sistemi di security management per le procedure applicative – Identity Access Management e Privileged Asset Management.....	11
5.1. Principi applicabili al legittimo trattamento dei dati.....	11
5.1.1. Erogazione servizi mediante protocollo HTTPS.....	12
5.1.2. Accessi al software mediante autenticazione multi fattore (MFA).....	12
5.1.3. Accessi al software protetti da nome utente e password.....	13
5.1.4. Password di accesso sicure.....	13
5.1.5. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.....	14
5.1.6. Protezione dei dati.....	15
5.1.7. Tracciabilità dei log di accesso	15
5.1.8. Tracciabilità delle variazioni ai dati del sistema	16
6. Erogazione servizio di assistenza remota.....	16
6.1.1. Collegamento da remoto	16
6.1.2. Accesso mediante utente "PAD_SUPPORT"	17
7. Subappalto di servizi - designazione degli ulteriori responsabili ex art. 28 GDPR	17
8. La restituzione dei dati a conclusione o revoca del contratto di Urbi Smart e WebTec.....	18
8.1. La restituzione dei dati a conclusione o revoca del contratto di conservazione digitale dei documenti informatici.....	18
ALLEGATO I - MISURE DI SICUREZZA IMPLEMENTATE E LIVELLI DI SERVIZIO.....	18
SUB 1 - REQUISITI DI CERTIFICAZIONE.....	18

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

<i>SUB 2 - CERTIFICAZIONI DEI DATA CENTER IN HOSTING</i>	19
<i>SUB 3 - MISURE DI SICUREZZA DI ALTO LIVELLO</i>	19
<i>SUB 4 - MISURE DI SICUREZZA DI DETTAGLIO</i>	21
<i>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)</i>	24
<i>5.1. Livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle infrastrutture digitali per la Pubblica Amministrazione</i>	24
<i>5.2. Livelli minimi di sicurezza e affidabilità servizio SAAS</i>	29
<i>SUB 6 - LIVELLI DI SERVIZIO</i>	31

CONFIDENZIALE

1. Inquadramento

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

Urbi Smart¹ 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 regolamentari² 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 Nazionale³ 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 e 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 ed Executive Order 12333.

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.). Inoltre, 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 1100 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 aggregazioni di Comuni, CST, Comunità Montane che vogliono erogare i servizi direttamente dalla loro server farm o struttura CED.

¹ URBI Smart e WebTec sono marchi distintivi che appartengono in esclusiva a PA Digitale

² la normativa applicabile è reperibile in appendice

³ 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>

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"⁴.

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 360.000 utenti finali e 90.000.000 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 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

⁴ <https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf>

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 Accredia⁵ 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 ISO/IEC 27035:2023).
- 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

⁵ 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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
- 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://conservatoriqualeficati.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-4975> e <https://www.acn.gov.it/portale/w/sa-4976>
- 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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), e 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, 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 adottato 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 cybersicurezza 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).

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 architetture 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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

Objective) compresi nel range inferiore a un'ora (salve dipendenze esterne non governabili da PA Digitale e dal fornitore IDC, 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 5.1. 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 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, OWASP, ecc.)
- 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 architettoniche 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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: rilocalazione 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 aggiuntivo 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 crittazione 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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 utilizzeranno 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 e 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.

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 e 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;
- 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 a 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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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.

- Erogazione servizio tramite protocollo https
- Accessi al software protetti da "nome utente" e "password".
- Password di accesso "sicure".
- Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.
- Protezione dei dati
- Tracciabilità dei log di accesso per eventuali comunicazioni di Data Breach.
- 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 mediante autenticazione multi fattore (MFA)

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 anche l'**autenticazione a due o più fattori**. L'autenticazione a due o più fattori, (conosciuta anche come strong authentication) è oggi il sistema di protezione più sicuro per proteggere i

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

propri account e una maggiore possibilità di controllo da parte dell'utente proprietario dell'account. Abbina alle credenziali (login, password), l'obbligo di confermare l'operazione attraverso smartphone o e-mail. 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 o più 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.

L'autenticazione a due o più fattori, infine, oltre ad essere una pratica raccomandata, è oggi un requisito obbligatorio in forza del Regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione, ai sensi dell'articolo 33-septies, comma 4, del Decreto-Legge 18 ottobre 2012, n. 179, convertito con modificazioni, dalla Legge 17 dicembre 2012, n. 221, adottato con Determinazione del Direttore dell'Agenzia per la Cybersicurezza Nazionale il 27 giugno 2024 (e s.m.i.). Tale requisito, in aggiunta, è obbligatorio anche nell'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 cybersicurezza 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).

5.1.3. Accessi al software protetti da nome utente e password

Come anticipato al paragrafo precedente, 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. In aggiunta all'autenticazione a due o più fattori, il sistema di autenticazione prevede altresì l'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.

5.1.4. 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)

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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).

5.1.5. 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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.

5.1.6. 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.

5.1.7. Tracciabilità dei log di accesso

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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.

5.1.8. 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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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 regola 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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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 (centottanta) 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
ISO 9001:2015	Sì	Sì	Non richiesto
ISO/IEC 27001:2013 oppure 27001:2022, con est. 27017:2015 e 27018.2019	Sì	Sì	Non richiesto
Per servizi critici: ISO 22301:2019	Sì	Sì	Non richiesto
Per servizi critici: ISO 20000-1:2020	Sì	Sì	Non richiesto

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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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_companyname_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 <i>Incident Management</i> , 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 <i>remediation plan</i> .
Misure di identificazione e autorizzazione dell'utente	Presenti soluzioni " <i>Privileged Access Management</i> " che consentono l'identificazione, l'autenticazione e processi di autorizzazione con disaccoppiamento dei privilegi amministrativi; Accesso remoto con autenticazione multifattoriale, ammesso esclusivamente da client

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

	<p>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.</p>
Misure di protezione dei dati durante la trasmissione	<p>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.</p>
Misure di protezione dei dati durante la conservazione	<p>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.</p>
Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati	<p>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;</p>
Misure per garantire la registrazione degli eventi	<p>Il Security Operation Center dei Data Centers 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.</p>
Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita	<p>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 <i>by design</i> e <i>by lifecycle</i> 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.</p>
Misure di informatica interna e di gestione e governance della sicurezza informatica	<p>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 al 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.</p>
Misure per garantire la conservazione limitata dei dati	<p>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</p>
Modalità per garantire l'assistenza al Titolare	<p>Esiste una disciplina contrattuale che impegna l'intera catena della fornitura a:</p> <ol style="list-style-type: none"> 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; consentire al Titolare del trattamento la verifica dei livelli di disponibilità;

	<p>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;</p> <p>c. garantire la formazione del proprio personale e l'assicurazione dell'impegno alla riservatezza, legalmente vincolante;</p> <p>d. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt.. Da 32 a 36 del GDPR ed in particolare:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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
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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

			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 rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.	ISO/IEC 27002:2022 7.4, 8.21 ISO/IEC 29100:2011 5.11 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 ETSI EN 319 401 clause 7.6

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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 ABCS 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
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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

			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
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 ABCS 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 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) e rinviando 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.

Classificazione dati: ordinari

Requisito
Affidabilità della soluzione complessiva
Alta affidabilità
A.AA-1: Disponibilità dell'infrastruttura
A.AA-2: Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità
Governance e processi
A.GP-1: I Servizi IT sono gestiti conformemente agli standard di settore
A.GP-2: È garantito il rispetto degli indicatori di servizio obbligatori
Performance e scalabilità
A.PS-1: Sono garantite caratteristiche minime di connettività

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

Sicurezza della componente applicativa
IDENTIFY (ID) Asset Management ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione ID.AM-3: I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati 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)
Governance ID.GV-1: È identificata e resa nota una policy di cybersecurity ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity
Risk Assessment ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
Supply Chain Risk Management 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
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 PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato PR.AC-3: L'accesso remoto alle risorse è amministrato 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 PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete) 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)
Awareness and Training PR.AT-1: Il personale del soggetto è informato e addestrato PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità
Data Security PR.DS-1: I dati memorizzati sono protetti PR.DS-2: I dati sono protetti durante la trasmissione PR.DS-3: Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak) PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
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) PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati 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 PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità
Maintenance PR.MA-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati
Protective Technology PR.PT-1: Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi 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
DETECT (DE) Anomalies and Events DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple
Security Continuous Monitoring DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity DE.CM-4: Il codice malevolo viene rilevato DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità
Detection Processes DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

RESPOND (RS) Mitigation RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato
Response Planning RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente
Communications RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente 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)
Analysis (RS.AN): 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)
RECOVER (RC) Recovery Planning (RC.RP): RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity
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 S.DC-02: Sono adottate misure di sicurezza fisica e ambientale
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
Capacità elaborativa
CE.CE-01: Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore
Risparmio energetico
RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore RE.GE-02: Valutazione annuale dell'efficienza energetica del Data Center
Affidabilità dell'infrastruttura digitale sottostante
Alta affidabilità A.AA-1: Disponibilità dell'infrastruttura A.AA-2: Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità
Governance e processi A.GP-1: I Servizi IT sono gestiti conformemente agli standard di settore A.GP-2: È garantito il rispetto degli indicatori di servizio obbligatori
Performance e scalabilità A.PS-1: Sono garantite caratteristiche minime di connettività
Business Continuity e Disaster Recovery A.BC-3: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti

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 99,6 % comprendendo i fermi programmati
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

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

SL6	Recovery Objective (RPO)	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).	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	data	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 Antincendio 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, mantenuti 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 <i>multi-carrier</i>).
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.

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

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-scavalco 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 anti-allagamento.
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 <i>adjustable long time</i> e <i>instantaneous trip</i> .
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 <i>Static Transfer Switch</i> e l' <i>Automatic Transfer Switch</i> , le <i>Power Distribution Unit</i> .
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 dal 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 dimensionati 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, <i>dry cooler</i> , 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 <i>Computer Room</i> 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 <i>Computer Room</i> ed <i>Entrance Room</i> con presenza di apparati attivi o sistema equivalente	Nelle computer Room e nell' <i>entrance room</i> l'impianto antincendio è usata la tecnologia VESDA o un sistema equivalente per la rilevazione dei fumi.
Spegnimento automatico a gas per <i>Computer Room</i> ed <i>Entrance Room</i> .	Nelle computer Room e nell' <i>entrance room</i> è presente un impianto per lo spegnimento automatico a gas, con la presenza di apparati attivi.
Sistema anti-allagamento per <i>Computer Room</i> ed <i>Entrance Room</i> con presenza di apparati attivi	Nelle <i>computer Room</i> e nell' <i>entrance room</i> è presente un impianto anti-allagamento, con la presenza di apparati attivi.

5.2. Livelli minimi di sicurezza e affidabilità servizio SAAS

Classificazione dati: ordinari

Requisito
Qualità del servizio (SLA) QU.SE-1: Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore QU.SE-2: Viene fornito un adeguato servizio di assistenza e supporto QU.SE-3: Il soggetto dichiara la frequenza di aggiornamento del servizio QU.SE-4: Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

<p>Livello del servizio (SLA) QU.LS-1: È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative QU.LS-2: Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione QU.LS-3: Esistono contenuti e caratteristiche minimi per i Service Level Agreement QU.LS-4: È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato.</p>
<p>Asset Management ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione ID.AM-3: I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati 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)</p>
<p>Governance ID.GV-1: È identificata e resa nota una policy di cybersecurity ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity</p>
<p>Risk Assessment ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio</p>
<p>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</p>
<p>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 PR.AC-3: L'accesso remoto alle risorse è amministrato 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 PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete) 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)</p>
<p>Awareness and Training PR.AT-1: Il personale del soggetto è informato e addestrato PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità</p>
<p>Data Security PR.DS-1: 1 dati memorizzati sono protetti PR.DS-2: I dati sono protetti durante la trasmissione PR.DS-3:11 trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak) PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione</p>
<p>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) PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati 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 PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità</p>
<p>Maintenance PR.MA-1: La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati</p>
<p>Protective Technology PR.PT-1; Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi 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</p>
<p>DETECT (DE) DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple DE.CM-1: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity DE.CM-4: Il codice malevolo viene rilevato DE.DP-1: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability</p>
<p>RESPOND (RS) RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente RS.CO-1: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente 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) RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne</p>

PA DIGITALE S.p.A. - Documento (C)onfidenziale - Autore PA Digitale S.p.A. - Ultima Revisione 2.02 del 15-05-2025 - È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale S.p.A. non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)

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 ⁶).	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

FINE DOCUMENTO

⁶ 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