Allegato n. 6 al Manuale del Sistema di Gestione Integrato

POLITICA DELLA CONTINUITÀ OPERATIVA

Revisione 03 del 26/05/2026

	EMESSO	APPROVATO
Funzione	**Responsabile Gestione Continuità Operativa**	**Amministratore Delegato**
Data	26/05/2026	26/05/2026
Firma		

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

INDICE

1. PREMESSA 3
2. SCOPO E CAMPO DI APPLICAZIONE 3
2.1 Scopo 3
2.2 Campo di Applicazione 3
3. CONCETTI FONDAMENTALI DELLA POLITICA DELLA CONTINUITÀ OPERATIVA 4
3.1 Contenuto della Politica 4
3.2 Responsabilità 7
3.3 Applicabilità 7
3.4 Riesame 7

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

1. PREMESSA

La Direzione ha definito la Politica per la Continuità Operativa e la comunica a tutte le parti interessate rilevanti attraverso la distribuzione del presente documento. La trasformazione dei concetti espressi nella Politica in una strategia aziendale avviene attraverso la definizione degli obiettivi annuali di Continuità Operativa. I concetti fondamentali della Politica della Continuità Operativa sono riportati al capitolo 3.

2. SCOPO E CAMPO DI APPLICAZIONE

2.1 Scopo

Scopo della presente Politica Aziendale è descrivere il Sistema di Gestione della Continuità Operativa (SGCO) della società PA DIGITALE S.p.A.

2.2 Campo di Applicazione

Oggetto del Sistema di Gestione per la Continuità Operativa:

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 dei servizi professionali connessi ai prodotti software. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza

Tutti i requisiti della Norma UNI EN ISO 22301:2019 (Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti) trovano applicazione nel Sistema di Gestione della Continuità Operativa (SGCO).
Nell'ambito del Sistema di Gestione Integrato aziendale, il Sistema di Gestione della Continuità Operativa di PA Digitale S.p.A. è integrato con i Sistemi di Gestione per la Qualità (UNI EN ISO 9001:2015), per la Sicurezza delle Informazioni (ISO/IEC 27001:2022, estesa alle Linee Guida ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27035:2023), per la Gestione dei Servizi IT (UNI CEI ISO/IEC 20000-1:2020), per la Salute e Sicurezza sul Luogo di Lavoro (UNI ISO 45001:***2023***), per l'Anticorruzione (UNI EN ISO 37001:***2025***).
Il Sistema di Gestione della Gestione della Continuità Operativa è stato pianificato in modo da considerare aspetti di Governance, Compliance, controlli interni e aspetti di Risk Management (con riferimento alle linee guida dello standard ISO 31000).

Il Sistema di Gestione della Continuità Operativa di PA Digitale S.p.A. è infine applicato secondo le seguenti normative vigenti:

- ***Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2), che abroga la Direttiva (UE) 2016/1148.***

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- ***Decreto legislativo 4 settembre 2024, n. 138, recante "Recepimento della direttiva (UE) 2022/2555 […] c.d. decreto NIS", che abroga il D.lgs. 18 maggio 2018, n. 65.***
- ***Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 379907 del 19 dicembre 2025 (in vigore dal 15 gennaio 2026), che stabilisce, in fase di prima applicazione, le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli artt. 23, 24, 25, 29 e 32 del decreto NIS – Allegato 2 "Misure di sicurezza di base per i soggetti essenziali" e Allegato 4 "Incidenti significativi di base per i soggetti essenziali".***
- ***Framework Nazionale per la Cybersecurity e la Data Protection, edizione 2025, elaborato dal CIS Sapienza e dal CINI in collaborazione con ACN.***

3. CONCETTI FONDAMENTALI DELLA POLITICA DELLA CONTINUITÀ OPERATIVA

3.1 Contenuto della Politica

Al fine di soddisfare con continuità le esigenze delle parti interessate rilevanti, PA Digitale S.p.A. ha definito e implementato un Sistema di Gestione della Continuità Operativa (SGCO), basato sui requisiti definiti dallo standard UNI EN ISO 22301:2019 sul perimetro specifico citato al capitolo 2.
PA Digitale opera da sempre nel settore informatico e ha piena consapevolezza dell'importanza che in questo settore riveste ad ogni livello la continuità operativa ("business continuity") e la resilienza di ogni singola organizzazione e di tutta la "supply chain".
A questo scopo PA Digitale applica "by design" e "by default" il rispetto dei requisiti contrattuali, cogenti e tecnici inerenti la continuità operativa nei processi e nei trattamenti delle informazioni correlati a tali processi. I requisiti per la continuità operativa diventano obiettivi aziendali; in particolare sono definiti, per ogni attività critica:

- Obiettivi minimi di continuità operativa (MBCO): livello minimo di servizi e/o prodotti accettabile per PA Digitale per raggiungere i propri obiettivi di business durante un'interruzione
- Obiettivi di massimo tollerabile periodo di interruzione (MTPD): tempo impiegato dagli impatti negativi, che potrebbero insorgere a causa di un'interruzione, per diventare intollerabili
- Obiettivo di tempo di recupero (RTO): periodo di tempo, dopo un incidente, entro cui il prodotto o il servizio deve essere ripristinato, o l'attività deve essere ripristinata, o le risorse devono essere recuperate
- Obiettivi di punto di recupero (RPO): punto in cui informazioni utilizzate da un'attività devono essere recuperate per consentire all'attività di riprendersi

In tale ottica si evidenzia l'impegno a mantenere e migliorare le competenze dei collaboratori, l'affidabilità dei processi e l'adeguatezza delle infrastrutture per essere sempre pronti a prevenire e, nel caso, a gestire interruzioni nella continuità operativa. PA Digitale tiene in grande considerazione, nella definizione delle proprie attività, le necessità e le aspettative delle parti interessate rilevanti. Relativamente ai Clienti, si impegna a

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

rispettare vincoli e requisiti esplicitati nella Business Impact Analisys condotta sui servizi in perimetro: il modello organizzativo è l'applicazione concreta dei principi di legalità, trasparenza, correttezza e lealtà che contraddistinguono da sempre i rapporti di PA Digitale con le parti interessate rilevanti. Nell'ambito del Sistema di Gestione della Continuità Operativa, l'azienda mira a realizzare i seguenti obiettivi strategici:

- garantire la continuità operativa e minimizzare gli impatti sul business in caso di crisi, salvaguardando sempre e comunque la salute e la sicurezza delle vite umane coinvolte e contemporaneamente assicurando:
  - la fornitura di prodotti e/o servizi a una capacità predefinita accettabile durante un'interruzione;
  - il rapido ripristino del normale stato di svolgimento delle attività di business;
- garantire la resilienza delle architetture;
- tutelare gli interessi aziendali e di Gruppo e aumentare la fiducia dei propri Clienti e Partner, ponendo particolare attenzione agli aspetti di:
  - disponibilità;
  - livello di servizio;
  - compliance.
- integrare gli obiettivi del Sistema di Gestione della Continuità Operativa con quelli dei Sistemi di Gestione implementati o in corso di implementazione, ovvero:
  - garantire la salvaguardia e la tutela delle vite umane a fronte di un evento di crisi. Il requisito della salvaguardia è quindi anche parte integrante della Politica per la Sicurezza (SGSSL) aziendale in conformità allo standard ISO 45001
  - garantire la resilienza nell'erogare servizi a fronte di incidenti (incluse situazioni di crisi o di emergenza generali) che possono portare all'interruzione dell'erogazione di tali servizi. Il requisito della continuità operativa è quindi parte integrante anche della Politica per la Qualità aziendale in conformità allo standard ISO 9001 e alla Politica per la Gestione dei Servizi IT aziendale in conformità allo standard ISO 20000-1
  - garantire la resilienza nel trattare dati personali in conformità ai requisiti del GDPR. Il requisito della continuità operativa è quindi anche parte integrante della Politica aziendale in materia di trattamento e protezione dei dati personali (in conformità al GDPR)
  - garantire la resilienza nel proteggere la sicurezza delle informazioni in conformità ai requisiti dello standard ISO 27001. Il requisito della resilienza è quindi anche parte integrante della Politica per la Sicurezza delle Informazioni aziendale in conformità allo standard ISO 27001
  - garantire la resilienza nel trattare dati personali in conformità ai requisiti di anticorruzione. Il requisito della continuità operativa è quindi anche parte integrante della Politica aziendale in materia di anticorruzione in conformità allo standard ISO 37001.

In linea con quanto definito dallo standard di riferimento, il top management di PA Digitale è attivamente coinvolto e impegnato nell'implementazione, mantenimento e miglioramento del Sistema di Gestione della Continuità Operativa (SGCO), mediante:

- definizione e formalizzazione di politiche per la continuità con precisi obiettivi, compatibili e coerenti con la direzione strategica dell'azienda;

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- definizione di un'analisi di impatto operativo (BIA), per identificare l'arco temporale oltre i quali gli impatti di un mancato recupero delle attività diventerebbero inaccettabili, individuando di conseguenza le attività prioritarie;
- definizione di una valutazione dei rischi di un'interruzione alle attività prioritarie;
- definizione di strategie e soluzioni per la continuità operativa, identificando le risorse necessarie all'attuazione di tali strategie e soluzioni;
- definizione di un piano di Business Continuity, che include anche quello di Disaster Recovery, che prevede test ripetuti per garantire l'adeguatezza e l'aggiornamento continuo delle strategie e soluzioni tecniche e organizzative adottate;
- definizione e formalizzazione di una struttura organizzativa, con ruoli e responsabilità precise in ambito di gestione della continuità, promuovendo il coinvolgimento di tutte le funzioni aziendali;
- comunicazioni al personale in merito alla necessità di soddisfare gli obiettivi, le politiche e i requisiti cogenti applicabili (leggi, regolamenti);
- pianificazione e assicurazione della disponibilità delle risorse umane e/o materiali;
- attività di formazione;
- monitoraggio delle performance e continuo miglioramento del sistema di gestione della continuità.

3.2 Conformità alla normativa NIS2 – continuità operativa e resilienza

PA Digitale S.p.A., in qualità di soggetto essenziale ai sensi dell'art. 6 del Decreto legislativo 4 settembre 2024, n. 138 (decreto NIS), è soggetta all'obbligo di adottare misure adeguate a garantire la continuità operativa e la resilienza dei propri servizi, ai sensi dell'art. 24 del decreto NIS e della misura ID.IM-04 dell'Allegato 2 della Determinazione ACN n. 379907/2025. La Politica della Continuità Operativa, basata sui requisiti della norma UNI EN ISO 22301:2019, costituisce il quadro di riferimento per l'attuazione di tale obbligo, integrando i requisiti NIS2 con quelli del Sistema di Gestione per la Continuità Operativa (SGCO).

I valori di RTO (Recovery Time Objective) e RPO (Recovery Point Objective) definiti in applicazione della presente Politica, sulla base degli esiti della Business Impact Analysis (POI SI 12), costituiscono i parametri minimi di resilienza operativa che PA Digitale S.p.A. si impegna a garantire ai propri clienti, anche ai fini del rispetto degli obblighi NIS2. La misura ID.IM-04 dell'Allegato 2 richiede che i piani di continuità operativa e di ripristino in caso di disastro siano approvati dagli organi di amministrazione e direzione, riesaminati almeno ogni due anni e aggiornati al verificarsi di incidenti significativi o di mutamenti dell'esposizione alle minacce. La presente Politica è approvata dall'Amministratore Delegato e sottoposta a riesame con la periodicità prevista, in conformità con tali requisiti.

Il Sistema di Gestione della Continuità Operativa di PA Digitale S.p.A. include, altresì, la gestione delle crisi informatiche prevista dalla misura ID.IM-04, punto 3, dell'Allegato 2, con definizione di ruoli, responsabilità e modalità di comunicazione con le Autorità competenti, inclusa l'Agenzia per la Cybersicurezza Nazionale (ACN).

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

3.3 Responsabilità

- DIREZIONE/AMMINISTRATORE DELEGATO. Ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di continuità operativa. Promuove la continuità operativa garantendo la congruità dei singoli budget destinati a tale scopo, coerentemente alle politiche e alle linee strategiche aziendali definite.
- RESPONSABILE DEL SISTEMA DI GESTIONE DELLA CONTINUITÀ OPERATIVA. Si occupa della progettazione, implementazione e conduzione del Sistema di Gestione della Continuità Operativa e in particolare di:
  - Assicurare che il sistema sia conforme ai requisiti della norma UNI EN ISO 22301:2019;
  - Riferire alla Direzione/Amministratore Delegato sulle prestazioni del Sistema di Gestione della Continuità Operativa.
- TUTTO IL PERSONALE che, a qualsiasi titolo, collabora con l'azienda, è responsabile dell'osservanza di questa policy e della segnalazione di anomalie di cui dovesse venire a conoscenza, anche non formalmente codificate, al Responsabile del Sistema di Gestione della Continuità Operativa.

3.4 Applicabilità

La presente Politica si applica indistintamente a tutti gli organi dell'azienda coinvolti nella:

- Erogazione del Software come Servizio - SaaS per il Mercato Pubblica Amministrazione e per il Mercato Privato
- Assistenza per i Servizi SaaS e Conservazione Digitale a Norma ed erogazione di servizi professionali
- Analisi, progettazione, sviluppo, produzione e manutenzione di Software erogati anche in modalità SaaS
- Erogazione del Software come Servizio - SaaS di Conservazione Digitale a Norma
- Commercializzazione e distribuzione di Software erogati anche in modalità SaaS

L'attuazione della presente Politica è obbligatoria per tutto il personale di PA Digitale.

3.5 Riesame

PA Digitale verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Continuità Operativa (SGCO), garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

La Politica Aziendale della Continuità Operativa qui descritta è soggetta a riesame in occasione del Riesame della Direzione e/o a seguito di cambiamenti significativi nel campo di applicabilità del Sistema di Gestione della Continuità Operativa in essere. In tale ambito viene verificata la conformità dei processi alle politiche di continuità operativa riportate nel presente documento, alle norme e ad altri requisiti di sicurezza appropriati all'ambito del Sistema di Gestione della Continuità Operativa (SGCO).

PA DIGITALE S.p.A. – Autore PA Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato – PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.