Allegato n. 3 al Manuale del Sistema di Gestione Integrato

POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI

Revisione 17 del 26/05/2026

	EMESSO	APPROVATO
Funzione	**Responsabile Gestione Sicurezza delle Informazioni**	**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. SCOPO, CAMPO DI APPLICAZIONE E PROFILO AZIENDALE 3
1.1 Scopo 3
1.2 Campo di Applicazione 3
1.3 Profilo aziendale 3
2. RIFERIMENTI 6
3. DEFINIZIONI 7
4. POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI 7
4.1 Motivazione 7
4.2 Obiettivi 9
4.3 Contenuto della Politica 9
4.3.1 Coinvolgimento e responsabilità delle risorse umane 10
4.3.2 Coinvolgimento della catena delle forniture 10
4.3.3 Organizzazione per la sicurezza 11
4.3.3.1 CYBERSECTEAM - STRUTTURA DI CYBERSECURITY DI GRUPPO 11
4.3.3.2 COMITATO AZIENDALE DI SICUREZZA INFORMATICA 12
4.3.3.3 INCARICATI PER LE COMUNICAZIONI CON LE AUTORITÀ 13
4.3.4 Controllo e classificazione delle risorse 13
4.3.5 Analisi dei rischi 14
4.3.6 Sicurezza e responsabilità del personale 15
4.3.7 Sicurezza della catena delle forniture 15
4.3.8 Sicurezza materiale e ambientale 16
4.3.9 Computer and Network Management 16
4.3.10 Controllo degli accessi 17
4.3.11 Scambio di informazioni 17
4.3.12 Sviluppo e manutenzione dei sistemi 18
4.3.13 Gestione della Business Continuity 18
4.3.14 Conformità legislativa 19
4.4 Responsabilità 19
4.5 Applicabilità 20
4.6 Riesame 20

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. SCOPO, CAMPO DI APPLICAZIONE E PROFILO AZIENDALE

1.1 Scopo

Scopo della presente Politica Aziendale è descrivere il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) della società PA DIGITALE S.p.A.

1.2 Campo di Applicazione

Oggetto del Sistema di Gestione per la Sicurezza delle Informazioni:

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 ISO/IEC 27001:2022 trovano applicazione nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Nel Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale S.p.A. trovano altresì applicazione le Linee Guida ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27035:2023. Infine, nell'ambito del Sistema di Gestione Integrato aziendale, il Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale S.p.A. è integrato con i Sistemi di Gestione per la Qualità (UNI EN ISO 9001:2015), per la Gestione dei Servizi IT (UNI CEI ISO/IEC 20000-1:2020), per la Continuità Operativa (UNI EN ISO 22301:2019), per la Salute e Sicurezza sul Luogo di Lavoro (UNI ISO 45001:***2023***), per l'Anticorruzione (UNI EN ISO 37001:***2025***).

1.3 Profilo aziendale

PA Digitale S.p.A. nasce nel 2009 per rispondere alle necessità di innovazione della Pubblica Amministrazione e alla spinta di accelerazione verso la digitalizzazione.
La completezza dell'offerta, la scelta strategica della tecnologia CLOUD COMPUTING - di seguito Cloud - definita anche SaaS (Software As A Service) o ASP (Application Service Providing), un tipo di approccio che valorizzi le esigenze dei clienti e la capacità di coordinare, gestire e realizzare progetti, permettono a PA Digitale di sviluppare prodotti e servizi di qualità che garantiscono all'ente di disporre di soluzioni software rispondenti all'evoluzione tecnologica e organizzativa della Pubblica Amministrazione e, dal 2014, anche per il mercato privato.
Pur mantenendo una forma giuridica indipendente, PA Digitale S.p.A. è soggetta a direzione e coordinamento di Gruppo Buffetti S.p.A., a sua volta parte del Gruppo che fa capo a Dylog Italia S.p.A., cui fanno capo alcune tra le più rinomate aziende del panorama industriale italiano, meglio illustrato nel company profile[1].

[1] https://www.dylog.it/aziende-del-gruppo/

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.

In passato, PA Digitale S.p.A. è stata la prima software house per la Pubblica Amministrazione in Italia ad essere iscritta nell'elenco dei Conservatori di documenti informatici dell'Agenzia per l'Italia Digitale, e oggi è tra le prime ad essere stata qualificata all'Elenco dei conservatori iscritti al Marketplace dei servizi di conservazione di AgID (https://conservatoriqualificati.agid.gov.it/), ai sensi delle Linee guida di cui all'art. 71 del CAD relative alla formazione, gestione e conservazione dei documenti informatici e del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici. L'Azienda è in grado di affiancare imprese, professionisti e pubbliche amministrazioni nei processi di conservazione digitale dei loro documenti informatici con un sistema di conservazione a norma, molto qualificato, governato e gestito da figure professionali capaci di garantire il costante aggiornamento e la conformità dei sistemi e dei processi all'evoluzione normativa e tecnologica.
L'Azienda segue attentamente lo sviluppo normativo della strategia cibernetica e del cloud nazionale, assumendo, come specifico mandato aziendale il perseguimento dei valori di servizio, per il consolidamento dell'evoluzione digitale del Paese, fondata su disponibilità di accesso non discriminante alle risorse digitali per i cittadini e le imprese, efficienza, efficacia, economicità e sicurezza, nel quadro delle regole comuni dettate dall'Ordinamento nazionale ed europeo.

La struttura organizzativa

Il personale di PA Digitale è altamente qualificato, con un'esperienza professionale ed elevate competenze specifiche nel mercato privato e della Pubblica Amministrazione Locale e Centrale.
L'azienda dispone di una infrastruttura informatica in grado di fornire un efficiente e puntuale supporto alle attività di progettazione, sviluppo, commercializzazione, manutenzione e assistenza dei prodotti software offerti.
PA Digitale è da sempre attenta a offrire servizi efficienti e professionali attraverso una struttura organizzativa che assicura:

- competenza e qualità nei processi di ingegneria di applicazioni e sistemi, con l'obiettivo di assicurare i requisiti funzionali nel rispetto dei principi di security e privacy by design e lungo l'intero ciclo di vita;
- competente supporto pre-vendita (analisi delle esigenze, studio della soluzione, ecc.);
- tempestivo e valido servizio post-vendita (installazione, avviamento, assistenza, ecc.);
- puntuale e completa formazione per utilizzare al meglio tutte le potenzialità delle proprie soluzioni;
- costante aggiornamento del software distribuito.

Nell'erogazione dei propri servizi e nel rispetto del principio di segregazione dei ruoli, PA Digitale S.p.A. adotta regole tassative per la gestione della propria catena delle forniture, con un approccio basato sul rischio. Al riguardo, la Società si avvale di fornitori di servizi cloud esterni, che soggiacciono alle regole di qualificazione stabilite nel quadro della "Strategia Cloud Italia", cui la stessa PA Digitale S.p.A. è soggetta, per assicurare un livello omogeneo di identificazione dei requisiti di sicurezza e continuità operativa, in aderenza ai principi ed agli obblighi stabiliti dall'Autorità di regolazione e vigilanza.
PA Digitale, inoltre, assume tra i propri obiettivi anche la partecipazione al sistema del "Polo Strategico Nazionale" per i servizi erogati dalle Pubbliche Amministrazioni, in ragione dei requisiti richiesti dal livello di criticità dei dati. Il Cloud Service Provider esterno,

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.

individuato tra i soggetti qualificati, deve possedere tutti i requisiti normativamente imposti e contrattualmente regolati da PA Digitale S.p.A. e periodicamente verificati a mezzo audit di prima o terza parte.

La rete commerciale

La rete commerciale è composta da un gruppo di funzionari addetti alla vendita diretta, oltre a una propria rete tecnico/commerciale composta da circa 30 partner con strutture complete e distribuite sull'intero territorio nazionale, per servizi commerciali, di avviamento, formazione, installazione e assistenza software.

L'offerta applicativa

PA Digitale vanta più di 1200 procedure software erogate in modalità SaaS oppure on premise presso circa 1000 clienti (Organi Costituzionali, Autorità indipendenti, Ministeri ed enti ministeriali, Regioni, Province, Comuni, Comunità montane, Unioni di Comuni, Consorzi, Enti Socio-Sanitari, Università, Enti Regionali, Soprintendenze, ecc.), e oltre 400.000 applicazioni erogate per clienti del mercato privato. La quasi totalità di questi clienti utilizza la Conservazione Digitale a Norma erogata da PA Digitale stessa.

Il contesto della presente politica è focalizzato su:

- Erogazione di soluzioni applicative (delle linee Urbi Smart e WebTec) in modalità sia SaaS che on premise (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), comprensiva di erogazione dei servizi professionali.
- Erogazione dei servizi SaaS in Cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.

COMPETENZE E ORGANIZZAZIONE

Le strutture della PA DIGITALE S.p.A. sono a:

- Pieve Fissiraga (LO) - Via Leonardo da Vinci n. 13: Sede Legale, Amministrativa e operativa
  - Direzione Generale (Amministratore Delegato)
  - ***Area Planning & Strategy***
  - ***Area Mercato Privato (comprendente Gestione Clienti Mercato Privato ed Help Desk Clienti Mercato Privato)***
  - Area Compliance e Privacy
  - Area Amministrazione e Contabilità
  - Area Affari Direzionali e Societari, Personale - Salute Sicurezza Lavoro - Finanza
  - ***Direzione Commerciale Mercato PA (comprendente Area Commerciale - Nord Est e Nord Ovest, Gare Pubbliche, Segreteria Commerciale Delivery Mercato Pubblica Amministrazione)***
  - ***Direzione Services & Partners Mercato PA (comprendente Product Marketing, Value Services, Project Management, Oikos Services, Servizi Documentali)***
  - ***Direzione ICT (comprendente Area Sistemistica Applicativa, Area Tecnica)***
  - ***Direzione Delivery Mercato PA***

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.

  - ***Area Software Factory - Prodotti Mercato Privato***

- Arezzo (AR) - Via Gobetti n. 21: Sede operativa
  - Area Commerciale Mercato PA (comprendente Area Commerciale - CENTRO)
  - Area Delivery Mercato PA
  - Area Software Factory

- Roma (RM) - Via Filippo Caruso, 23: Sede operativa (*)
  - Area Delivery Mercato PA
  - ***Area Services and Partners***

- ***Torino (TO) - Corso Bramante, 53: Sede operativa (*)***
  - ***Area Services and Partners***

- Napoli (NA) - Via G. Porzio n. 4 Centro Direzionale Isola E3 - 7° piano: - Sede operativa
  - Area Commerciale Mercato PA (comprendente Area Commerciale - SUD e Roma-PAC)
  - Area Delivery Mercato PA
  - Area Software Factory
  - Area Amministrazione e Contabilità

PA Digitale, inoltre, si avvale della struttura di Cybersecurity di Gruppo, per garantire la sicurezza delle informazioni, dei sistemi e delle reti, secondo i principi normativi, regolamentari e di politica interna stabiliti in modo vincolante per le Società del Gruppo.

(*) ***Le Sedi fisiche di Roma e Torino sono le uniche sedi*** non interessata dal Sistema di Gestione della Sicurezza delle Informazioni. Sui processi inerenti il servizio di Conservazione Digitale a Norma (in particolare nel servizio di assistenza) operano addetti in tutte le sedi (Roma esclusa).

2. RIFERIMENTI

La presente politica descrive gli elementi del Sistema di Gestione della Sicurezza delle Informazioni in conformità alla Norma ISO/IEC 27001:2022 e recepisce - facendoli propri - i contenuti della Politica per la Sicurezza delle Informazioni del Gruppo Buffetti-Dylog (controllante di PA Digitale S.p.A.). Alla presente politica sono altresì correlate:

- la Politica aziendale per la Gestione degli Incidenti di Sicurezza delle Informazioni
- la Politica di Sicurezza per il Modello di Responsabilità Condivisa (Shared Security Responsibility Model) – SSRM

La presente politica, nello specifico delle più recenti novità normative, è anche riferita a:

- ***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. DEFINIZIONI

Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)
Quella parte del sistema di gestione complessivo, basata su un approccio rivolto al rischio relativo al business, volta a stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornato e migliorare la sicurezza delle informazioni.
Nota: Il sistema di gestione include la struttura organizzativa, le politiche, le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi e le risorse.

Sicurezza delle Informazioni
Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

Riservatezza
Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati

Integrità
Proprietà relativa alla salvaguardia dell'accuratezza e della completezza dei beni.

Disponibilità
Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

4. POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI

4.1 Motivazione

PA Digitale S.p.A. è un'Azienda che eroga soluzioni legate all'Information technology, e in particolare ha realizzato:

- Erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi Smart) e per il mercato privato (della linea WebTec)
- un Servizio di Conservazione Digitale a Norma dei Documenti Informatici.

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.

Le soluzioni sopra indicate sono declinate nel Piano di Gestione dei Servizi istituito per la norma UNI CEI ISO/IEC 20000-1:2020, ovvero:

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

Data la natura delle proprie attività, e vista la Normativa vigente per quanto concerne l'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale e Servizi di Conservazione Digitale dei Documenti a Norma per le Pubbliche Amministrazioni e per il mercato privato, PA Digitale S.p.A. considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del patrimonio informativo dei propri clienti e un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo. Inoltre, pone particolare attenzione ai temi riguardanti la sicurezza durante l'erogazione del servizio, che deve essere ritenuto un bene primario dell'azienda. Il SGSI si applica a tutte le attività di:

- Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi Smart), comprensiva di erogazione dei servizi professionali
- Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per il mercato privato (della linea WebTec), comprensiva di erogazione dei servizi professionali
- Analisi, progettazione, messa in esercizio ed esercizio stesso del Servizio di Conservazione Digitale a Norma e dei dati ad esso collegato, nonché ai servizi di assistenza al cliente.

In particolare, cura la tutela dell'accesso ai sistemi sia fisici che logici.
Consapevole del fatto che l'erogazione dei servizi per soggetti esterni può comportare l'affidamento di dati e informazioni critiche, l'unità organizzativa che si occupa della progettazione ed erogazione di tali servizi opera secondo normative di sicurezza internazionalmente riconosciute.
Per questi motivi si intendono adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità del patrimonio informativo affidato a PA Digitale S.p.A. dai propri Clienti.
Su tale linea PA Digitale S.p.A. ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento, in conformità anche alle indicazioni della norma ISO/IEC 27001:2022, nonché alle Linee Guida ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27035:2023.

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.

4.2 Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale è di garantire un adeguato livello di sicurezza dei dati e delle informazioni attraverso l'identificazione, la valutazione e il trattamento dei rischi a cui i propri servizi e le proprie soluzioni sono soggette, nell'ambito del campo di applicazione sopra indicato, finalizzata al continuo miglioramento, secondo un processo ciclico che coinvolge l'intera organizzazione e si estende ai fornitori.
Il Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- Integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre, con la presente politica PA Digitale intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Proteggere il patrimonio informativo dei propri clienti;
- Evitare al meglio ritardi nel rilascio dei servizi erogati;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua crescita professionale;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza;
- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente.

4.3 Contenuto della Politica

Il SGSI si applica a tutte le attività di erogazione dei servizi legati:

- all'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi Smart)
- all'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per il mercato privato (della linea WebTec)
- al Servizio di Conservazione Digitale a Norma

e ai dati ad essi collegati.

Tutte le informazioni che vengono create o utilizzate dall'Azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

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.

La Politica della Sicurezza delle Informazioni adottata da PA Digitale deve costituire un approccio sistematico alla sicurezza delle informazioni per tutti i componenti dell'organizzazione che - a qualsiasi titolo - possono intervenire su qualsiasi informazione presente all'interno dell'Azienda, nell'ambito del campo di applicazione sopra indicato. Per quanto la Politica della Sicurezza delle Informazioni, essa si basa sui principi fondamentali di seguito descritti.

Per quanto riguarda in modo specifico il trattamento dei dati personali, si rimanda alla Politica in materia di trattamento e protezione dei dati personali.

L'erogazione dei Servizi in modalità Cloud Computing (Servizi SaaS e Servizio di Conservazione Digitale a Norma) è basata sull'infrastruttura fornita da un Internet Data Center gestito da un Fornitore esterno i cui siti risiedono sul territorio nazionale. La Politica Aziendale della Sicurezza di PA Digitale prevede che tale Fornitore abbia a sua volta una certificazione ISO/IEC 27001:2013 o ISO/IEC 27001:2022 (nonché alle Linee Guida ISO/IEC 27017:2015, ISO/IEC 27018:2019) nell'ambito del servizio di data center fornito a PA Digitale, e che la filiera dei suoi eventuali fornitori sia monitorata, come previsto dalla Politica di Sicurezza per il Modello di Responsabilità Condivisa (Shared Security Responsibility Model) - SSRM.

4.3.1 Coinvolgimento e responsabilità delle risorse umane

Il SGSI deve essere pienamente recepito, accettato e compreso da tutto il personale in organico in azienda, senza alcuna esclusione. Tale coinvolgimento è necessario perché, nell'ambito di azione dell'organizzazione, ogni collaboratore non solo può entrare in contatto con alcune o tutte le informazioni custodite e trattate dall'azienda, ma comunque può prendere visione e conoscere i meccanismi di sicurezza e protezione di PA Digitale nell'ambito del campo di applicazione sopra indicato. PA Digitale adotta pertanto le seguenti linee guida:

- attivazione di processi di formazione periodici per tutto il personale coinvolto, in materia di:
  - riservatezza e confidenzialità delle informazioni;
  - politiche aziendali e di Gruppo per la sicurezza;
  - procedure interne;
  - normative vigenti.
- creazione di un ambiente consapevole dell'importanza della sicurezza e dei rischi relativi, attraverso l'impegno diretto dei responsabili aziendali;
- adozione di strumenti di diffusione e aggiornamento indiretti, tramite l'uso del sistema informatico di bacheca aziendale e del Sistema Documentale interno.

4.3.2 Coinvolgimento della catena delle forniture

I principi del SGSI devono essere condivisi e partecipati alla catena delle forniture, attraverso un processo di identificazione dei fornitori critici ed una condivisione delle regole e degli obiettivi di sicurezza attesi, che devono entrare all'interno dei vincoli contrattuali, quale presupposto di validità e parametro di misura dell'adempimento delle prestazioni attese.

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.

La gestione della catena delle forniture è attuata sulla base dei principi di gestione del rischio, applicando logiche di priorità, parametri di misura e valutazione dei criteri di efficacia, inserendo il processo di gestione dei fornitori all'interno dei domini di rischio e di continuità operativa.

4.3.3 Organizzazione per la sicurezza

Per poter governare il SGSI, PA Digitale, nell'ambito del campo di applicazione sopra indicato, definisce e istituisce al proprio interno una specifica organizzazione.

Tale organizzazione si articola su tre livelli:
- il CyberSecTeam - Struttura di Cybersecurity di Gruppo
- il Comitato aziendale di Sicurezza Informatica
- gli incaricati per le comunicazioni con le Autorità

4.3.3.1 CyberSecTeam - Struttura di Cybersecurity di Gruppo

Recependo le indicazioni del Gruppo controllante, PA Digitale ha incorporato nel proprio organigramma aziendale (come entità esterna) il CyberSecTeam - Struttura di Cybersecurity di Gruppo, la cui missione è assicurare il soddisfacimento dei requisiti di sicurezza delle informazioni, dei sistemi e delle reti, in aderenza agli standard internazionali di settore, per la costituzione, il mantenimento e lo sviluppo di un Information Security Management System, con valenza di Gruppo e con progressiva attuazione a tutte le società, in attuazione della Security e Privacy Policy e le attività collegate alla tutela dei dati personali. Tale struttura, nei confronti di PA Digitale, ha il ruolo di guida e revisione del Sistema di Gestione di Sicurezza delle Informazioni già implementato, e risulta così composta:

Componente	Advisor di Gruppo per le aree IT e Cybersecurity Buffetti S.p.A.
Componente	Head of Cybersecurity EDIST S.r.l.

Insieme con i membri del CyberSecTeam sopra elencati, possono intervenire anche altri componenti incaricati dall'Advisor di Gruppo per le aree IT e Cybersecurity Buffetti S.p.A. (ad es. Data Protection Team di Gruppo o specialisti in materia di sicurezza delle informazioni).

La struttura dipende direttamente dal Vertice della Capogruppo ed ha le seguenti responsabilità:
- Garantire lo sviluppo e il mantenimento del Security Management System, monitorandone l'attuazione da parte delle strutture titolari dei processi di competenza, curando la coerenza di processo anche relativamente agli obblighi di privacy e delle altre normative di settore applicabili per singoli domini;
- Assicurare, a livello di Gruppo, l'attuazione dei processi del Security Management System, curando l'analisi, la valutazione e la gestione dei rischi e degli eventi relativi alla sicurezza delle informazioni, dei sistemi e delle reti e dei fattori fisici, ambientali e umani rilevanti;
- Curare la definizione dei requisiti e delle policy di security delle informazioni, dei sistemi e delle reti, verificandone l'applicazione attraverso controlli di secondo livello (security survey e verifiche di sicurezza), identificando e valutando i rischi derivanti

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.

dall'introduzione di modifiche o di nuove implementazioni ai sistemi tecnologici e alle reti;
- Avviare e sviluppare i processi di monitoraggio real-time, near-real-time degli eventi;
- Gestire eventi e incidenti di sicurezza garantendo i coordinamenti con il personale del Gruppo e con tutte le strutture di Gruppo che erogano servizi informativi;
- Raccogliere e gestire lo scambio di informazioni inerenti vulnerabilità software o indicatori di compromissione, con enti istituzionali o componenti private attive nel sistema di Cyber Threat Intelligence, e curare i rapporti con le Autorità di settore;
- Avviare e consolidare un processo di presidio di sicurezza dei sistemi e delle reti individuando vulnerabilità e contromisure di contenimento e ripristino, proponendo soluzioni ai fini del mantenimento e miglioramento dei livelli di security stabiliti;
- Stabilire i principi e le regole operative dei processi di Identity Access Management (IAM), curando le verifiche di secondo livello relative all'identificazione e all'accesso ai sistemi;
- Definire policy e linee guida per la protezione delle informazioni, dei sistemi e delle reti e dei dati personali delle strutture di Gruppo interessate nei processi di sviluppo software e per gli elementi di cybersecurity nella catena degli approvvigionamenti, verificandone l'applicazione attraverso controlli di secondo livello;
- Attuare i processi del Sistema di Gestione della Sicurezza delle Informazioni secondo la norma di standardizzazione (ISO 27001), anche attraverso l'analisi delle occorrenze, la determinazione delle contromisure e la diffusione delle lezioni apprese;
- Curare, con le strutture competenti di Capogruppo e delle Società interessate, la formazione del personale a tutti i livelli, la promozione della cultura della security;
- Fornire il contributo specialistico per le evoluzioni di mercato di prodotti e servizi, nello sviluppo di nuove opportunità;
- Relativamente allo specifico impegno verso PA Digitale S.p.A., contribuire alla revisione del Sistema di Gestione per la Sicurezza delle Informazioni esistente, oltreché degli attuali Sistemi di Gestione attualmente adottati dalla Società integrati con il predetto Sistema di Gestione per la Sicurezza delle Informazioni

A tale struttura riportano direttamente sia il Responsabile per la Gestione della Sicurezza delle Informazioni che il Comitato aziendale di Sicurezza Informatica. Posso riportare anche i Responsabili di Area individuati come Risk Owners, Asset Owners e/o Task Owners.

4.3.3.2 Comitato aziendale di Sicurezza Informatica

Internamente, in PA Digitale opera una struttura trasversale alle Aree aziendali di Organigramma, denominata Comitato di Sicurezza Informatica e composta da almeno un rappresentante delle Aree aziendali che hanno impatto sulla sicurezza delle informazioni:

Presidente del Comitato	Amministratore Delegato
Componente	Direttore ICT
Componente	Operatore Area Tecnica
Componente	Responsabile Produzione Software Factory
Componente	Responsabile del Servizio di Conservazione
Componente	Responsabile dello Sviluppo del Sistema di Conservazione
Componente	Responsabile per la Gestione della Sicurezza delle Informazioni

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.

L'organizzazione interna ha i seguenti obiettivi, in accordo con il CyberSecTeam - Struttura di Cybersecurity di Gruppo:

- controllare la sicurezza delle informazioni in seno all'organizzazione;
- supportare il processo di identificazione delle vulnerabilità e delle minacce;
- verificare l'attuazione dei controlli selezionati;
- sovrintendere i processi e le attività legate alla sicurezza;
- definire le modalità per il monitoraggio e la revisione del SGSI;
- farsi carico dei processi di mantenimento, evoluzione e miglioramento del sistema.

Le linee guida per la istituzione e l'operatività di tale organizzazione sono:

- individuazione dei componenti della struttura nell'ambito della direzione e delle figure chiave aziendali, anche in base alla preparazione e all'esperienza (Comitato di Sicurezza Informatica, come sopra definito);
- inserimento di almeno un elemento esterno;
- contatto con organizzazioni ed enti di riferimento per la problematica;
- utilizzo costante degli strumenti operativi (riunioni, comunicazioni interne, ecc.) tali da rendere attivo e propositivo il lavoro del Gruppo.

4.3.3.3 Incaricati per le comunicazioni con le Autorità

Per rispondere ai crescenti requisiti normativi ***(tra cui la Determina ACN n. 307/2022 e ss.mm.ii.)***, in particolar modo legati alla necessità di definire e rendere noti i ruoli e le responsabilità inerenti alla cybersecurity per tutto il personale e per le terze parti rilevanti (es. fornitori, clienti, partner), PA Digitale ha nominato:

- un incaricato (e il suo sostituto), con il compito di gestire l'attuazione delle disposizioni normative in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico dell'azienda e assicura l'efficace implementazione delle misure di sicurezza
- un referente tecnico (e il suo sostituto), in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia.

Tale struttura è di seguito declinata:

Incaricato	Advisor di Gruppo per le aree IT e Cybersecurity Buffetti S.p.A.
Sostituto	Responsabile per la Gestione della Sicurezza delle Informazioni PA Digitale S.p.A.
Referente Tecnico	Direttore ICT di PA Digitale S.p.A.
Sostituto	Responsabile dello Sviluppo del Sistema di Conservazione PA Digitale S.p.A.

4.3.3.4 Incaricati per le comunicazioni con lo CSIRT Italia

Conformemente con il quadro normativo attualmente vigente, in merito alla gestione degli incidenti significativi, e più in generale per le comunicazioni in materia con le Autorità ad essa deputate, PA Digitale ha nominato:

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.

Referente CSIRT	***Direttore ICT di PA Digitale S.p.A.***
Sostituto	***Advisor di Gruppo per le aree IT e Cybersecurity Buffetti S.p.A.***

4.3.4 Controllo e classificazione delle risorse

Per una corretta attuazione del SGSI è necessaria un'appropriata classificazione delle risorse, in modo da garantirne l'appropriato controllo e la precisa individuazione dei relativi livelli di protezione. La classificazione delle risorse avviene a partire dall'analisi dei processi aziendali, in modo da individuarle e classificarle in base alle informazioni entro-contenute. Tale controllo deve rispettare le seguenti linee guida sottoindicate.

Classificazione delle informazioni trattate in azienda, individuate sulla base dell'analisi dei processi aziendali (segnatamente entro il dominio di applicazione del SGSI), in modo da individuare, controllare e classificare le seguenti tipologie di risorse:

1 Asset Processi Aziendali (principali);
2 Asset informazioni (secondari);
3 Asset fisici (secondari);
4 Asset informatici (secondari);
5 Asset personale (secondari).

Linee guida:

- La classificazione degli Asset è a cura del Responsabile Area Tecnica, del Responsabile della Sicurezza Informatica e del Responsabile Gestione Sicurezza delle Informazioni;
- L'aggiornamento dell'elenco degli Asset deve avvenire ad ogni variazione;
- Il Responsabile Gestione Sicurezza delle Informazioni si assicura che l'elenco degli Asset sia sempre aggiornato.

Il controllo degli Asset deve essere effettuato in maniera incrociata, tra l'analisi dei processi aziendali coinvolti nell'ambito del SGSI e l'inventario diretto dei beni e delle risorse.

4.3.5 Analisi dei rischi

Relativamente all'ambito del SGSI, tale sistema deve prevedere - in conformità alla norma ISO/IEC 27001:2022 - che sia condotta con frequenza almeno annuale un'analisi dei rischi, che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti.

Tale analisi sarà ponderata anche rispetto al valore di business degli Asset principali e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

L'analisi dei rischi viene effettuata sugli Asset principali attraverso l'analisi sugli Asset secondari ad essi collegati.

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.

4.3.6 Sicurezza e responsabilità del personale

Gli obiettivi che PA Digitale intende raggiungere attraverso la responsabilizzazione del personale sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture dell'organizzazione coinvolte nell'ambito del SGSI;
- accertarsi che gli utenti interni siano informati sulle minacce alla sicurezza delle informazioni e siano formati a sostenere le politiche di sicurezza aziendali nel corso della propria attività lavorativa;
- minimizzare il danno per incidenti e malfunzionamenti circa la sicurezza e mettere a frutto l'esperienza di avvenimenti precedenti.

Le linee guida sono:

- individuare il personale direttamente coinvolto nei trattamenti delle informazioni, nell'uso e nella gestione delle risorse incluse nel dominio del SGSI;
- selezionare nuove figure, se necessario;
- verificarne l'adeguatezza;
- definire e rendere evidenti a tutte le persone coinvolte le modalità di accesso alle informazioni, i controlli e le registrazioni di tali accessi.

Inoltre, si rende necessario imporre il rispetto delle regole in maniera tassativa, per tutti coloro che in PA Digitale hanno accesso, a qualsiasi titolo, ai dati presenti in azienda e correlati all'ambito di applicazione del SGSI, inclusi quindi gli eventuali responsabili, gli incaricati, o qualsiasi fornitore o terza parte esterna.

4.3.7 Sicurezza della catena delle forniture

È istituito, mantenuto e aggiornato un sub-processo di gestione della catena delle forniture, che declina i principi di gestione della sicurezza nei riguardi dei fornitori, con particolare riferimento a quelli che assumono un ruolo rilevante o critico nei processi di erogazione dei servizi agli utenti pubblici e privati, ovvero a funzioni indirette che possano impattare sugli obiettivi della Società.

In applicazione dei principi del framework nazionale, gli obiettivi che PA Digitale persegue nei riguardi dei fornitori sono:

- identificare i rischi che attengono alla catena delle forniture e gestirli, avendo cura di garantire il rispetto dei requisiti normativi, regolamentari e di contratto;
- assicurarsi che i fornitori siano consapevoli del loro ruolo e responsabilità, come intrinseco presupposto della relazione contrattuale e a garanzia degli interessi del Paese, dei cittadini, degli utenti qualificati e delle imprese che contrattualmente si affidano ai servizi di PA Digitale;
- assicurare che il nesso fiduciario che deve legare il fornitore a PA Digitale venga sorretto da evidenze e verifiche, in un rapporto leale di collaborazione basato su evidenze oggettive e dimostrabili lungo tutto il ciclo di vita delle relazioni contrattuali.

Le linee guida sono:

- identificare i requisiti legali e contrattuali e parteciparli al fornitore sin dalle fasi di iniziativa precontrattuale

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.

- chiarire il ruolo del fornitore nel processo di fornitura ed ottenerne la piena consapevolezza e responsabilizzazione;
- attuare, mediante le appropriate misure contrattuali, i processi di attuazione dei principi e delle regole, della conseguente verifica, applicare i correttivi che necessitino all'occorrenza ovvero i rimedi contrattuali e legali specifici;
- esporre agli utenti e alle autorità di vigilanza, in maniera trasparente, le relazioni connesse alla catena delle forniture:
- misurare la qualità ed efficacia delle relazioni interne alla catena delle forniture.

L'adesione ai principi e alle regole del SGSI applicabili, da parte dei fornitori, è condizione necessaria e presupposto giuridico dei contratti.

4.3.8 Sicurezza materiale e ambientale

Gli obiettivi di PA Digitale sono:

- impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni di "business";
- impedire la perdita, i danni ai beni del sistema e la interruzione delle attività economiche;
- impedire la manomissione o il furto delle informazioni. Devono essere adottate misure di sicurezza di natura fisica, tecnica ed elettronica delle quali venga resa evidenza nelle procedure attuative del SGSI;
- avvalersi di Certification Authority riconosciute per quanto riguarda soluzioni di crittografia utilizzate per accedere ai dati tramite interfaccia web based.

Per la definizione e l'attuazione di tali misure gli elementi di riferimento adottati sono:

- progettazione e realizzazione di ambienti, impianti e dispositivi di prevenzione rispetto a furti, incendi, calamità, ecc.; a tal fine PA Digitale fa ricorso a progettisti specializzati in materia e/o fornitori esterni anch'essi certificati ISO/IEC 27001:2013 o ISO/IEC 27001:2022;
- rispetto di tutte le normative e regolamenti vigenti in materia;
- definizione di controlli periodici adeguati sugli impianti, sui locali e sui dispositivi tali da garantirne la continuità e il miglioramento nel tempo;
- sistemi di allarme, controllo e autorizzazione degli accessi che permettano la gestione di zone e aree differenziate all'interno dell'organizzazione;
- progettazione e implementazione di sistemi informatici - e uso di appropriati apparati complementari - in grado di garantire continuità di funzionamento anche in caso di guasti improvvisi prevedendo, ad esempio, apparati "fault tolerant", alimentazione ridondante, gruppi di continuità e gruppi elettrogeni. A tal proposito PA Digitale fa sempre ricorso a progettisti e ingegneri qualificati in materia e/o a fornitori esterni anch'essi certificati ISO/IEC 27001:2013 o ISO/IEC 27001:2022.

Le variazioni e le modifiche vengono sempre notificate per tempo a tutti i responsabili coinvolti in modo da generare una adeguata circolazione e condivisione delle modifiche alla struttura e alle misure di sicurezza.

4.3.9 Computer and Network Management

Gli obiettivi e le linee guida adottate sono:

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.

- assicurare il corretto e sicuro funzionamento delle funzioni di elaborazione delle informazioni;
- minimizzare il rischio di guasti dei sistemi;
- proteggere l'integrità del software e delle informazioni;
- gestire l'integrità e la disponibilità dei processi di elaborazione dell'informazione e della comunicazione;
- garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di supporto;
- prevenire i danni ai servizi e le interruzioni alle attività economiche;
- evitare la perdita, modifica o abuso delle informazioni scambiate tra le organizzazioni.

4.3.10 Controllo degli accessi

Gli obiettivi e le linee guida adottate sono:

- controllare l'accesso alle informazioni;
- assicurare la protezione dei servizi in rete;
- prevenire l'accesso non autorizzato ai sistemi;
- rilevare attività non autorizzate;
- garantire la sicurezza delle informazioni quando sono utilizzate dalle postazioni mobili in servizi di rete e telematici.

PA Digitale definisce e organizza al proprio interno articolati sistemi di autenticazione e di gestione dei permessi di accesso ai sistemi, prevedendo il riconoscimento sia delle eventuali postazioni di lavoro usate per l'accesso automatico a tali sistemi sia del personale incaricato dell'attività.
In quest'ambito sono previsti sistemi di documentazione degli accessi che consentano l'identificazione di anomalie e non sono ammessi programmi di utilities potenzialmente in grado di annullare i controlli dei sistemi e delle applicazioni. Inoltre, le sessioni inattive sono disattivate automaticamente dopo un determinato periodo di inattività e sono poste limitazioni automatiche ai tempi di connessione per fornire sicurezza aggiuntiva alle applicazioni ad alto rischio che erogano:

- soluzioni applicative di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi Smart), erogate anche in modalità SaaS
- soluzioni applicative di prodotti software per il mercato privato (della linea WebTec), erogate anche in modalità SaaS
- il Servizio di Conservazione Digitale a Norma

4.3.11 Scambio di informazioni

PA Digitale adotta una politica selettiva per lo scambio di informazioni, in particolare verso l'esterno. A tal proposito ha provveduto a classificare le informazioni e a determinare le modalità e gli strumenti di scambio, per ogni classe di informazione. L'obiettivo di tale attività è quello di mantenere la sicurezza delle informazioni e del software scambiati all'interno dell'organizzazioni e con entità esterne. Nell'ambito del Servizio di Conservazione Digitale a Norma non è previsto l'utilizzo di supporti rimovibili. L'accesso alle informazioni avviene tramite sistema web based e anche al termine dei contratti in essere con i clienti, il materiale può essere scaricato dal sistema, senza l'utilizzo di media rimovibili quali a titolo di esempio CD, DVD o altro.

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.

4.3.12 Sviluppo e manutenzione dei sistemi

Gli obiettivi sono:
- garantire che la sicurezza sia applicata correttamente in tutti sistemi in funzione;
- garantire il corretto uso, dimensionamento, controllo e manutenzione di tutti sistemi in esercizio;
- prevenire la perdita, modifica o cattivo utilizzo dei dati nei sistemi applicativi;
- proteggere la riservatezza, autenticità e integrità dell'informazione;
- assicurare che attività sul software utilizzato per l'erogazione del servizio e attività di supporto siano condotte in modo sicuro;
- gestire la sicurezza del software e dei dati di sistema.

Ai fini della corretta gestione di questa fase, l'azienda implementa procedure organizzative che consentano la regolare applicazione di tutte le idonee soluzioni di sicurezza e di dimensionamento, sia preventive che correttive. Sono inoltre previste politiche di evoluzione del sistema SGSI che definiscono obiettivi e controlli significativi e applicabili all'organizzazione del sistema.

Le linee guida definite in tale area sono:
- analisi e progettazione di architetture e sistemi condivise con tutte le funzioni aziendali coinvolte e con il ricorso a specialisti preventivamente selezionati;
- definizione di adeguate procedure e regole di sicurezza per la gestione dei controlli di accesso ai sistemi dall'interno e dall'esterno della rete, della protezione fisica e logica dei sistemi con tutti gli strumenti disponibili allo stato dell'arte della tecnologia;
- ricorso a politiche di backup complete e diversificate per garantire la ridondanza delle informazioni salvate;
- implementazione di idonee soluzioni di "disaster recovery";
- definizione di adeguate procedure e regole di sicurezza per la gestione dei controlli e della supervisione di reti e sistemi;
- divieto di utilizzo di mobile code;
- azione preventiva per l'individuazione, la definizione e la gestione di procedure di analisi, progettazione, sviluppo e manutenzione del software prodotto internamente alla struttura;
- definizione e impiego di appropriate politiche di screening, valutazione e test per la selezione e l'accettazione di soluzioni software e di sistema;
- definizione e aggiornamento di un piano di capacità del servizio.

4.3.13 Gestione della Business Continuity

È uno dei termini fondamentali e PA Digitale lo recepisce appieno e fa proprio nell'ambito del sistema SGSI, dato che l'azienda deve mantenere pienamente efficienti ed efficaci tutti i servizi a disposizione dei propri Clienti nell'ambito di applicabilità del SGSI medesimo. La Business Continuity è quindi interpretata non solo come strumento per la massimizzazione dei propri risultati economici, ma ancor più come elemento alla base dei servizi erogati ai clienti e pertanto vitale per il funzionamento dell'azienda stessa, oltre che come elemento per ridurre al minimo i possibili rischi di contenzioso legale con i propri clienti. Gli obiettivi sono di contrastare le interruzioni delle attività di servizio e dei processi di servizio critici, dagli effetti di malfunzionamenti, interruzioni, guasti o disastri.

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.

Per una corretta applicazione della Business Continuity, PA Digitale ha adottato un sistema di Gestione per la Continuità Operativa che definisce al proprio interno dei processi per la gestione della medesima (dettati dalle norme UNI EN ISO 22301:2019 e UNI EN ISO 22313:2020), dei piani strategici per l'approccio dei rischi e l'analisi degli impatti, lo sviluppo e il mantenimento di specifici piani di continuità operativa. Infine, definisce le modalità di verifica, correzione e ridefinizione dei piani di business continuity.

4.3.14 Conformità legislativa

Come già esplicitato nei punti precedenti, le linee guida sono:

- garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari;
- garantire il rispetto dei termini contrattuali stabiliti con i propri clienti;
- garantire il rispetto di specifiche norme adottate obbligatoriamente o volontariamente da PA Digitale.

La legislazione europea e italiana è stringente soprattutto per tutto ciò che riguarda la gestione della privacy che, nell'ambito in cui opera PA Digitale è intesa sia come gestione della privacy per tutti i dati che riguardano i propri dipendenti, clienti e fornitori, sia per tutti i dati trattati e archiviati in nome e per conto dei propri clienti. Per questo motivo PA Digitale ha predisposto una opportuna Politica in materia di trattamento e protezione dei dati personali, pubblicata sul sito www.padigitale.it.

Rispetto della legge e dei principi di legalità, correttezza e trasparenza
L'azienda intende rispondere all'esigenza di assicurare condizioni di trasparenza nella conduzione della propria attività, alle legittime aspettative dei soci, di tutte le parti interessate e del lavoro dei propri dipendenti, alle necessarie tutele della propria posizione e immagine, mediante l'adozione del Modello di Organizzazione, Gestione e Controllo previsto dal Decreto Legislativo 8 giugno 2001, n 231 e del relativo Codice Etico (conformi alle linee guida di Confindustria) quale espressione dei valori e dei principi che ispirano e guidano l'attività aziendale. Tali strumenti, pubblicati sul sito www.padigitale.it, devono rappresentare validi veicoli di sensibilizzazione di tutti coloro che agiscono in nome o comunque nell'interesse dell'Azienda, affinché, conformando costantemente il loro operare alle prescrizioni ivi previste, ispirino e orientino i loro comportamenti al rispetto della legge e dei principi di legalità, correttezza e trasparenza.

4.4 Responsabilità

- 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 Sicurezza delle Informazioni.
- 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 sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget destinati alla sicurezza coerentemente alle politiche e alle linee strategiche aziendali definite.

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.

- RESPONSABILE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI. Si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni e in particolare di:
  - Assicurare che il sistema sia conforme ai requisiti della norma ISO/IEC 27001:2022 esteso alle Linee Guida ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 27035:2023;
  - Riferire alla Direzione/Amministratore Delegato e al CyberSecTeam - Struttura di Cybersecurity di Gruppo sulle prestazioni del Sistema di Gestione per la Sicurezza delle Informazioni.
- TUTTI I SOGGETTI ESTERNI sono tenuti al rispetto dei principi del SGSI applicabili. Inoltre, coloro che potrebbero avere accesso alle informazioni riservate devono garantire il rispetto dei requisiti di sicurezza attraverso la sottoscrizione di un "accordo di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

4.5 Applicabilità

Ferma restando l'applicabilità per via contrattuale ai fornitori dei principi e delle regole del SGSI, la presente Politica si applica indistintamente a tutti gli organi dell'Azienda coinvolti:

- nei processi di analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi Smart), comprensiva di erogazione dei servizi professionali;
- nei processi di analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per il mercato privato (della linea WebTec), comprensiva di erogazione dei servizi professionali;
- nell'erogazione del Servizio di Conservazione Digitale a Norma e del relativo servizio di assistenza.

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

PA Digitale consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali, che devono avvenire nel rispetto delle regole e delle norme cogenti.

4.6 Riesame

PA Digitale verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, 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 Sicurezza 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 Sicurezza delle Informazioni in essere. In tale ambito viene verificata la conformità dei processi di elaborazione delle informazioni

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.

rispetto alle politiche di sicurezza riportate nel presente documento, alle norme e ad altri requisiti di sicurezza appropriati all'ambito del SGSI.7.

4.7 Conformità alla normativa NIS2 – qualifica di soggetto essenziale

PA Digitale S.p.A. è classificata come soggetto essenziale ai sensi dell'art. 6 del Decreto legislativo 4 settembre 2024, n. 138 (decreto NIS), che recepisce la Direttiva (UE) 2022/2555 (NIS2) nell'ordinamento nazionale. In tale qualità, la Società è assoggettata agli obblighi di cui agli artt. 23, 24 e 25 del decreto NIS, con il livello di vigilanza rafforzata previsto per i soggetti essenziali ai sensi dell'art. 36 del medesimo decreto.
La presente Politica Aziendale della Sicurezza delle Informazioni, in coerenza con il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato ISO/IEC 27001:2022, costituisce il quadro di riferimento per l'attuazione delle misure di sicurezza di base previste dall'Allegato 2 della Determinazione del Direttore Generale ACN n. 379907 del 19 dicembre 2025 (in vigore dal 15 gennaio 2026). Le misure adottate sono organizzate secondo le funzioni GV (Govern), ID (Identify), PR (Protect), DE (Detect), RS (Respond) e RC (Recover) del Framework Nazionale per la Cybersecurity e la Data Protection, edizione 2025, in linea con i requisiti del medesimo Allegato 2.
L'Organizzazione per la Sicurezza Informatica di PA Digitale S.p.A., descritta al paragrafo 4.3.3 della presente Politica, svolge le funzioni dell'organizzazione per la sicurezza informatica richiesta dalla misura GV.RR-02 dell'Allegato 2, includendo il punto di contatto, il referente CSIRT e i rispettivi sostituti, come previsto dall'art. 7, comma 6, del decreto NIS. La presente Politica è approvata dagli organi di amministrazione e direzione ai sensi dell'art. 23 del decreto NIS e della misura GV.PO-01 dell'Allegato 2, che richiede l'approvazione e la comunicazione delle politiche di sicurezza informatica agli organi competenti.
La presente Politica è sottoposta a riesame almeno annuale, al verificarsi di incidenti significativi e al mutare dell'esposizione alle minacce, in conformità con la misura GV.PO-02 dell'Allegato 2 e con l'art. 24 del decreto NIS. La documentazione relativa alle misure adottate e agli esiti del riesame è conservata e resa disponibile per le attività di supervisione e vigilanza dell'Agenzia per la Cybersicurezza Nazionale (ACN) ai sensi degli artt. 37 e seguenti del decreto NIS.

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.