Pa33 S.r.l.

POLITICA PER LA QUALITÀ E LA SICUREZZA INFORMATICA

Documento a disposizione delle parti interessate

Norme di riferimento del Sistema di Gestione Integrato:

EN ISO 9001:2015 • ISO/IEC 27001:2024 • ISO/IEC 27701:2019
ISO/IEC 27017:2021 • ISO/IEC 27018:2020

Rev.	Data	Descrizione	Approvato
00	10 marzo 2020	Prima emissione	Amministratore
01	10 marzo 2026	Versione estesa per le parti interessate	Amministratore

1. Presentazione dell'organizzazione

Pa33 S.r.l. è una società italiana di consulenza e sviluppo software, fondata con l'obiettivo di accompagnare la Pubblica Amministrazione e il settore privato nei processi di innovazione digitale e conformità normativa.

Le attività principali di Pa33 comprendono:

- la produzione di software gestionali e soluzioni applicative offerte anche in modalità SaaS (Software as a Service) ad enti pubblici e privati in genere;
- la progettazione e l'erogazione di corsi di formazione per enti pubblici e privati.

Le piattaforme SaaS di Pa33 sono qualificate nel Catalogo dell'Agenzia per la Cybersicurezza Nazionale (ACN), a conferma del rispetto degli standard di sicurezza richiesti per i servizi destinati alla Pubblica Amministrazione italiana.

Pa33 opera in conformità a un Sistema di Gestione Integrato (SGI) certificato secondo le norme EN ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2020, esteso con l'implementazione della ISO/IEC 27701:2019 per la gestione della privacy.

2. Scopo e destinatari della politica

La presente politica definisce i principi, gli impegni e gli obiettivi strategici di Pa33 S.r.l. in materia di qualità dei prodotti e dei servizi e di sicurezza delle informazioni, intesa in senso ampio come protezione delle informazioni, sicurezza informatica e tutela dei dati personali.

Il documento è rivolto a tutte le parti interessate dell'organizzazione:

- clienti, sia della Pubblica Amministrazione sia del settore privato;
- dipendenti e collaboratori di Pa33;
- fornitori e partner tecnologici;
- autorità regolatorie e di vigilanza (Agenzia per la Cybersicurezza Nazionale, Garante per la Protezione dei Dati Personali, AgID);
- organismi di certificazione;
- comunità e territorio.

La politica è coerente con la missione, la visione e la direzione strategica dell'organizzazione. Essa fornisce il quadro di riferimento per la definizione degli obiettivi annuali ed è riesaminata periodicamente dall'Alta Direzione per assicurarne la continua idoneità.

3. Missione e visione

3.1 Missione

Fornire alla Pubblica Amministrazione e al settore privato soluzioni software innovative, sicure e conformi alla normativa, accompagnando i nostri clienti nella trasformazione digitale con competenza, trasparenza e continuo miglioramento.

3.2 Visione

Essere il partner di riferimento per la compliance e l'innovazione digitale nel Mezzogiorno d'Italia e oltre, distinguendoci per la qualità dei servizi, la sicurezza dei dati e l'integrità professionale.

3.3 Valori

- Qualità: perseguiamo l'eccellenza in ogni prodotto e servizio che forniamo;
- Sicurezza: proteggiamo le informazioni dei nostri clienti come se fossero le nostre;
- Trasparenza: comunichiamo con chiarezza e onestà con tutte le parti interessate;
- Innovazione: investiamo continuamente in tecnologia e competenze;
- Conformità: operiamo nel pieno rispetto delle normative nazionali, europee e internazionali;
- Responsabilità: rispondiamo dei nostri impegni e delle nostre azioni.

4. Impegni per la qualità

L'Alta Direzione di Pa33 S.r.l. si impegna a:

4.1 Soddisfazione del cliente

Comprendere e soddisfare le esigenze esplicite e implicite dei clienti, puntando al superamento delle loro aspettative. La soddisfazione è misurata sistematicamente attraverso questionari, analisi dei reclami e feedback, e i risultati sono utilizzati come input per il miglioramento continuo.

4.2 Conformità dei prodotti e dei servizi

Garantire che i prodotti software e i servizi di formazione siano conformi alle specifiche concordate, ai requisiti cogenti e regolamentari applicabili e alle migliori pratiche del settore. I processi di sviluppo software seguono metodologie strutturate che integrano i principi di quality assurance, testing sistematico e validazione.

4.3 Approccio per processi

Gestire le attività dell'organizzazione come un sistema di processi interconnessi, ciascuno con input, output, responsabilità e indicatori di prestazione definiti. L'approccio per processi consente di ottimizzare le risorse, ridurre gli sprechi e garantire la ripetibilità dei risultati.

4.4 Competenza e valorizzazione delle persone

Investire nella formazione continua e nella crescita professionale del personale, riconoscendo che le competenze delle persone sono il principale fattore di qualità. Il piano di formazione annuale copre competenze tecniche, normative, metodologiche e trasversali.

4.5 Gestione dei fornitori

Selezionare, valutare e monitorare i fornitori secondo criteri documentati, assicurando che contribuiscano al raggiungimento degli obiettivi di qualità e sicurezza. I fornitori critici sono sottoposti a valutazioni periodiche e ad obblighi contrattuali specifici.

4.6 Miglioramento continuo

Perseguire il miglioramento continuo dell'efficacia del Sistema di Gestione Integrato attraverso l'analisi dei dati, gli audit interni, il riesame della direzione, la gestione delle non conformità e delle azioni correttive, e il recepimento delle innovazioni tecnologiche e normative.

5. Impegni per la sicurezza delle informazioni

Pa33 S.r.l., consapevole del valore strategico delle informazioni e della fiducia che i clienti ripongono nell'organizzazione, si impegna a proteggere il patrimonio informativo secondo i più elevati standard internazionali.

5.1 Principi fondamentali

La sicurezza delle informazioni in Pa33 è fondata su tre principi cardine:

- Riservatezza: le informazioni sono accessibili esclusivamente alle persone autorizzate, in base al principio del need-to-know e del least privilege;
- Integrità: le informazioni sono accurate, complete e protette da alterazioni non autorizzate, accidentali o deliberate;
- Disponibilità: le informazioni e i servizi sono accessibili quando necessario, con livelli di servizio definiti e monitorati.

A questi si aggiungono i principi di autenticità (verifica dell'identità di utenti e sistemi) e di non ripudio (tracciabilità e attribuibilità delle azioni).

5.2 Gestione del rischio

Pa33 adotta un approccio sistematico alla gestione del rischio per la sicurezza delle informazioni, conforme alla clausola 6.1 della ISO/IEC 27001:2022. I rischi sono identificati, analizzati, valutati e trattati attraverso un processo documentato che tiene conto delle minacce emergenti, delle vulnerabilità dei sistemi e dell'impatto potenziale sulle attività dell'organizzazione e sui diritti degli interessati.

I controlli di sicurezza sono selezionati dall'Annex A della ISO/IEC 27001:2022 e dalle estensioni delle ISO/IEC 27017, 27018 e 27701 sulla base dell'analisi del rischio. La loro applicabilità e le relative giustificazioni sono documentate nella Statement of Applicability.

5.3 Sicurezza dei servizi cloud

In qualità di Cloud Service Provider, Pa33 adotta i controlli aggiuntivi previsti dalla ISO/IEC 27017:2021 per garantire la sicurezza dei servizi cloud, tra cui:

- segregazione logica dei dati tra i diversi clienti (multi-tenancy sicuro);
- definizione chiara delle responsabilità condivise tra Pa33 (CSP) e il cliente (CSC);
- trasparenza sulla localizzazione dei dati, sulle misure di sicurezza adottate e sui sub-processori coinvolti;
- supporto alla portabilità dei dati e all'interoperabilità;
- monitoraggio continuo dei servizi e gestione proattiva delle vulnerabilità;
- crittografia dei dati in transito e a riposo con algoritmi conformi agli standard di settore.

5.4 Gestione degli incidenti

Pa33 dispone di procedure strutturate per la rilevazione, la gestione, la notifica e l'analisi degli incidenti di sicurezza delle informazioni. In caso di incidente, l'organizzazione attiva il processo di incident response, che comprende il contenimento dell'impatto, la risoluzione, la comunicazione tempestiva alle parti interessate e l'analisi post-incidente per l'identificazione delle lezioni apprese.

5.5 Continuità operativa

Pa33 mantiene piani di continuità operativa e di disaster recovery per garantire la ripresa dei servizi critici entro tempi definiti (RTO/RPO). I piani sono testati periodicamente e aggiornati sulla base dei risultati dei test e delle evoluzioni dell'infrastruttura.

5.6 Consapevolezza e formazione

Tutto il personale riceve formazione periodica sulla sicurezza delle informazioni, comprendente: principi di sicurezza, riconoscimento delle minacce (phishing, social engineering), gestione delle credenziali, segnalazione degli incidenti, obblighi di riservatezza. L'efficacia della formazione è verificata attraverso test e simulazioni.

6. Impegni per la protezione dei dati personali

Pa33 S.r.l. ha implementato un Privacy Information Management System (PIMS) conforme alla ISO/IEC 27701:2019 e al Regolamento (UE) 2016/679 (GDPR). La protezione dei dati personali è parte integrante del Sistema di Gestione Integrato e permea tutte le attività dell'organizzazione.

6.1 Ruoli nel trattamento dei dati personali

Pa33 opera in un duplice ruolo:

- come Titolare del trattamento (PII Controller) per i dati personali dei propri dipendenti, collaboratori, contatti commerciali e candidati;
- come Responsabile del trattamento (PII Processor) per i dati personali dei clienti trattati attraverso le piattaforme SaaS.

Per ciascun ruolo, Pa33 applica i controlli specifici previsti dalla ISO/IEC 27701 (Annex A per il Titolare, Annex B per il Responsabile) e dal GDPR.

6.2 Principi di protezione dei dati

Il trattamento dei dati personali in Pa33 si fonda sui seguenti principi:

- liceità, correttezza e trasparenza: ogni trattamento ha una base giuridica documentata e gli interessati ricevono informative chiare e complete;
- limitazione della finalità: i dati sono raccolti per finalità determinate, esplicite e legittime e non sono trattati per finalità incompatibili;
- minimizzazione: sono trattati esclusivamente i dati personali strettamente necessari per la finalità perseguita;
- esattezza: i dati sono mantenuti aggiornati e accurati;
- limitazione della conservazione: i dati sono conservati per il tempo strettamente necessario e cancellati o anonimizzati al termine;
- integrità e riservatezza: i dati sono protetti con misure tecniche e organizzative adeguate al rischio;
- accountability: Pa33 è in grado di dimostrare in ogni momento la conformità ai principi sopra enunciati.

6.3 Privacy by design e by default

La protezione dei dati personali è integrata fin dalla fase di progettazione di ogni prodotto, servizio e processo dell'organizzazione. Le impostazioni predefinite di ogni sistema garantiscono il massimo

livello di protezione della privacy. In particolare, nella progettazione delle piattaforme SaaS, Pa33 adotta: minimizzazione dei dati raccolti, pseudonimizzazione ove possibile, isolamento dei dati tra tenant, configurabilità dei periodi di conservazione, supporto nativo ai diritti degli interessati.

6.4 Diritti degli interessati

Pa33 garantisce l'esercizio di tutti i diritti riconosciuti dal GDPR agli interessati:

- diritto di accesso ai propri dati personali;
- diritto di rettifica dei dati inesatti o incompleti;
- diritto alla cancellazione ("diritto all'oblio");
- diritto alla limitazione del trattamento;
- diritto alla portabilità dei dati;
- diritto di opposizione al trattamento;
- diritto a non essere sottoposto a decisioni basate unicamente su trattamenti automatizzati.

Le richieste sono gestite attraverso una procedura strutturata che assicura la risposta entro i termini di legge. Per i dati trattati come Responsabile, Pa33 assiste tempestivamente il Titolare nella gestione delle richieste.

6.5 Trattamento dei dati nel cloud

Per i servizi SaaS, Pa33 adotta i controlli previsti dalla ISO/IEC 27018:2020 per la protezione dei dati personali nel cloud:

- i dati personali sono trattati esclusivamente secondo le istruzioni documentate del Titolare;
- i dati non sono utilizzati da Pa33 per finalità proprie (marketing, profilazione, analytics);
- i sub-processori sono utilizzati solo con l'autorizzazione preventiva del Titolare e con garanzie contrattuali equivalenti;
- i dati sono conservati su infrastrutture all'interno dello Spazio Economico Europeo;
- al termine del rapporto contrattuale, i dati sono restituiti e/o cancellati secondo le istruzioni del Titolare;
- le violazioni dei dati personali sono notificate al Titolare senza ingiustificato ritardo.

6.6 Data Protection Officer

Pa33 ha designato un Data Protection Officer (DPO), quale punto di contatto per gli interessati, per il Garante per la Protezione dei Dati Personali e per le questioni interne relative alla privacy. Il DPO supervisiona il PIMS, fornisce pareri sulle valutazioni d'impatto (DPIA) e verifica la conformità dell'organizzazione alla normativa sulla protezione dei dati.

7. Conformità normativa e quadro di riferimento

Il Sistema di Gestione Integrato di Pa33 è conforme alle seguenti norme e regolamentazioni:

7.1 Norme ISO

- EN ISO 9001:2015 — Sistemi di gestione per la qualità — Requisiti;
- ISO/IEC 27001:2022 — Sicurezza delle informazioni, cybersecurity e protezione della privacy — ISMS — Requisiti;
- ISO/IEC 27701:2019 — Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni sulla privacy (PIMS);

- ISO/IEC 27017:2021 — Codice di condotta per i controlli di sicurezza per i servizi cloud;
- ISO/IEC 27018:2020 — Codice di condotta per la protezione delle PII nei cloud pubblici.

7.2 Normativa europea e nazionale

- Regolamento (UE) 2016/679 (GDPR) — Protezione dei dati personali;
- D.Lgs. 196/2003 e s.m.i. — Codice in materia di protezione dei dati personali;
- D.Lgs. 138/2024 — Recepimento della Direttiva (UE) 2022/2555 (NIS2);
- Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.);
- Regolamento ACN per la qualificazione dei servizi cloud per la PA.

7.3 Certificazioni e qualificazioni

Pa33 S.r.l. è certificata ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 20000. I servizi SaaS sono qualificati nel Catalogo ACN con elevati standard di sicurezza. L'organizzazione ha inoltre implementato il PIMS conforme alla ISO/IEC 27701 ed è in fase di certificazione.

8. Obiettivi strategici

Coerentemente con la presente politica, l'Alta Direzione definisce annualmente obiettivi misurabili per la qualità e la sicurezza delle informazioni. Gli obiettivi sono comunicati a tutto il personale, monitorati trimestralmente e riesaminati in sede di riesame della direzione.

I principali ambiti degli obiettivi sono:

Qualità dei servizi

- disponibilità dei servizi SaaS (uptime target);
- tempi di risposta e risoluzione del supporto tecnico;
- soddisfazione del cliente;
- conformità dei prodotti alle specifiche.

Sicurezza delle informazioni

- numero e gravità degli incidenti di sicurezza;
- tempi di rilevazione e risposta;
- esito delle scansioni di vulnerabilità;
- completamento del piano di trattamento dei rischi.

Protezione dei dati personali

- tempi di risposta alle richieste degli interessati;
- completamento delle DPIA per i trattamenti ad alto rischio;
- conformità del registro dei trattamenti;
- numero di violazioni dei dati personali.

Miglioramento organizzativo

- completamento del piano di formazione;
- esiti degli audit interni;
- tasso di chiusura delle non conformità e delle azioni correttive.

9. Responsabilità

L'attuazione della presente politica è responsabilità di tutti coloro che operano in nome o per conto di Pa33 S.r.l. I principali ruoli sono:

- l'Alta Direzione è responsabile della definizione, dell'approvazione e del riesame della politica, dell'allocazione delle risorse necessarie e della promozione della cultura della qualità e della sicurezza;
- il Responsabile del SGI (RSGI) coordina l'attuazione operativa del sistema, la gestione della documentazione, il monitoraggio dei KPI e la pianificazione degli audit;
- il CISO (Chief Information Security Officer) supervisiona la sicurezza delle informazioni, gestisce il rischio informatico e coordina la risposta agli incidenti;
- il DPO (Data Protection Officer) supervisiona la conformità alla normativa sulla protezione dei dati personali e il funzionamento del PIMS;
- i responsabili di funzione attuano la politica nelle rispettive aree di competenza;
- tutto il personale e i collaboratori si conformano alla presente politica e alle procedure del SGI.

Le violazioni della presente politica possono comportare provvedimenti disciplinari e/o contrattuali proporzionati alla gravità della violazione.

10. Comunicazione, disponibilità e riesame

10.1 Comunicazione interna

La presente politica è comunicata a tutto il personale e ai collaboratori di Pa33 al momento dell'assunzione o dell'inizio della collaborazione, e in occasione di ogni aggiornamento. È sempre disponibile nella documentazione interna del SGI e nell'area riservata della intranet aziendale.

10.2 Disponibilità alle parti interessate

La presente politica è resa disponibile alle parti interessate esterne nei seguenti modi:

- pubblicazione sul sito web istituzionale di Pa33 S.r.l.;
- consegna ai clienti su richiesta e in fase di qualificazione commerciale;
- trasmissione agli organismi di certificazione;
- consegna ai fornitori nell'ambito del processo di qualificazione;
- messa a disposizione delle autorità regolatorie su richiesta.

10.3 Riesame periodico

La politica è riesaminata dall'Alta Direzione almeno una volta all'anno, in sede di riesame della direzione, e in ogni caso quando si verifichino:

- modifiche significative al contesto interno o esterno dell'organizzazione;
- modifiche alla normativa applicabile;
- risultati di audit interni o esterni che ne evidenzino l'inadeguatezza;
- incidenti significativi di sicurezza o violazioni dei dati;
- feedback rilevanti da parte delle parti interessate.

Le modifiche sono approvate dall'Alta Direzione e comunicate tempestivamente a tutte le parti interessate.

Dichiarazione dell'Alta Direzione

Con la presente politica, l'Alta Direzione di Pa33 S.r.l. conferma il proprio impegno a:

- soddisfare i requisiti dei clienti e delle parti interessate, mirando al superamento delle loro aspettative;
- proteggere le informazioni e i dati personali affidati all'organizzazione con le migliori misure tecniche e organizzative disponibili;
- rispettare tutti i requisiti legali, regolamentari e contrattuali applicabili;
- perseguire il miglioramento continuo del Sistema di Gestione Integrato;
- fornire le risorse necessarie per il raggiungimento degli obiettivi definiti;
- promuovere la cultura della qualità, della sicurezza e della protezione dei dati a tutti i livelli dell'organizzazione.

La presente politica è vincolante per l'intera organizzazione e rappresenta l'impegno formale dell'Alta Direzione nei confronti di tutte le parti interessate.