POLITICA PER LA QUALITÀ E PER LA SICUREZZA DELLE INFORMAZIONI

REVISIONI

N. Rev.	Data Rev.	Descrizione	Redazione	Verifica	Approvazione
1	01.06.2023	Revisione generale dei contenuti	RSGI	Strutture interessate	RSGI

Premessa

La Fondazione Enpam definisce e documenta la propria Politica per la Qualità e per la Sicurezza delle informazioni in ottemperanza alla normativa di settore (UNI EN ISO 9001:2015, in seguito ISO 9001, e UNI EN ISO 27001:2013, in seguito ISO 27001).

Con l'obiettivo di ancorare la gestione dei propri processi aziendali a standard di qualità riconosciuti secondo la normativa ISO 9001, la Fondazione Enpam ha istituito, con delibera del CdA n. 42/2010, il Sistema di Gestione per la Qualità. Il Servizio Sistemi di Gestione Aziendale e di Controllo, della struttura Processi e Controllo, gestisce e manutiene il Sistema di gestione per la Qualità, secondo le linee di indirizzo definite dalla Direzione Generale, con la piena e fattiva collaborazione delle strutture e dei responsabili di Servizi, Strutture e Aree della Fondazione.

Nel 2018, la Fondazione ha volontariamente intrapreso il percorso per conformarsi anche alla norma ISO che disciplina la Sicurezza delle informazioni sulla base dello standard 27001:2013. L'obiettivo dello standard ISO 27001:2013 è quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato Sistema di gestione della Sicurezza delle Informazioni finalizzato ad una corretta gestione dei dati dell'azienda. Il Servizio Sicurezza delle Informazioni e Controllo dei Processi IT, della struttura Processi e Controllo, gestisce e manutiene il Sistema di Gestione per la Sicurezza delle Informazioni.

La Fondazione ha inoltre ritenuto necessario rafforzare il presidio sulla compliance al Regolamento Generale sulla Protezione dei Dati Personali (Regolamento (UE) 2016/679 – GDPR) istituendo l'Ufficio Protezione Dati, che supporta il DPO nell'esecuzione dei suoi compiti e integrando il Sistema di Gestione della Sicurezza delle Informazioni (ISO/IEC 27001) con i requisiti della norma ISO/IEC 27701:2019 per la gestione delle informazioni sulla privacy.

Riguardo tale tematica si rimanda al documento "Politica per la Protezione dati Personali" pubblicato nella sezione "Privacy" del sito web della Fondazione.

Con l'adozione di tale Sistema la Fondazione si è dunque dotata di un evoluto Sistema Integrato di Gestione per la Qualità, per la Sicurezza delle informazioni e per la Privacy.

Il Sistema di gestione integrato è coordinato dal Servizio Sistemi di Gestione Aziendale e di Controllo, della struttura Processi e Controllo.

La Fondazione opera secondo un approccio per processi e, nell'ambito di tale approccio, utilizza la metodologia "plan-do-check-act", basandosi sul criterio "risk based thinking".

Campo di applicazione del Sistema di gestione integrato

I requisiti del sistema di gestione integrato si applicano, con riferimento alla ISO 9001, ai seguenti processi: attività di assistenza agli iscritti, investimenti patrimoniali e relative attività di controllo. processo relazioni con il pubblico, processo gestione degli investimenti e relativi controlli, processo di acquisto e appalto in qualità di stazione appaltante ed a tutti i processi di supporto (gestione delle risorse umane, sistemi informatici ed infrastrutture, gestione amministrativa e contabile, comunicazione, …). I requisiti tecnico-organizzativi di sicurezza delle informazioni riferiti alla ISO 27001 si applicano a tutti i processi della Fondazione.

Mission istituzionale

La Fondazione ha lo scopo di attuare la previdenza e l'assistenza a favore degli iscritti, dei loro familiari e superstiti, nonché di realizzare interventi di promozione e sostegno all'attività e al reddito dei professionisti iscritti, secondo quanto previsto dalla legge e dai regolamenti deliberati dalla Fondazione medesima ed approvati dalle

Amministrazioni vigilanti di cui all'art. 3 del decreto legislativo 30 giugno 1994, n. 509. (art 2 dello Statuto).

Nell'assolvere tale compito, la Fondazione persegue obiettivi di stabilità, solidità, sostenibilità, solidarietà ed equità intergenerazionale, promuovendo un sistema previdenziale ed assistenziale che tuteli gli iscritti sia al raggiungimento della pensione sia lungo l'attività professionale.

Obiettivi strategici della Fondazione

L'Enpam individua i seguenti obiettivi strategici, che ne guidano l'operato.

1. Sensibilità al rischio aziendale

Obiettivo della Fondazione è implementare, gestire e manutenere un efficace sistema di gestione dei rischi.

Il processo di gestione del rischio adottato dall'Ente recepisce i principi e le linee guida desunti dalla UNI ISO 31000:2018, attraverso lo sviluppo delle seguenti fasi:

- mappatura dei processi attuati dall'amministrazione;
- valutazione del rischio per ciascun processo;
- trattamento del rischio identificato.

Il sistema Control & Risk Self Assessment (CRSA), adottato dalla Fondazione, ha come obiettivo quello di migliorare la cultura del controllo a tutti i livelli manageriali ed operativi, e di ottemperare alla normativa in materia (Codice civile - D.Lgs. n. 231/2001). Tale metodologia prevede una autovalutazione dei rischi e dei controlli effettuata da tutto il management aziendale, con la guida di un soggetto (c.d. "facilitatore", in Enpam la figura del Comitato di controllo interno), il cui ruolo è quello di assicurare sistematicità al processo.

La Fondazione Enpam esegue, inoltre, una valutazione del rischio relativo alla sicurezza delle informazioni relative ai propri iscritti.

Tale valutazione viene effettuata periodicamente e comunque a seguito di cambiamenti significativi che modifichino gli scenari di riferimento.

I rischi di sicurezza individuati sono trattati ed opportunamente gestiti attraverso un Piano di trattamento del rischio che mantiene traccia degli stessi e delle informazioni relative a:

- le attività di intervento necessarie a mitigare il rischio;
- gli owner del rischio;
- il responsabile dell'intervento attuativo;
- le tempistiche previste.

2. Interesse degli iscritti

La Fondazione mira alla piena e continua soddisfazione dei propri iscritti, tutelandone gli interessi anche attraverso il costante studio e perfezionamento di strumenti atti a soddisfarne le necessità; si impegna inoltre a fornire trasparente e puntuale comunicazione della propria gestione, anche in ottemperanza alla vigente normativa sulla Trasparenza e con il solo limite della riservatezza stabilita dalle leggi e dai regolamenti[1].

La Fondazione Enpam si impegna a garantire che tutte le esigenze implicite ed esplicite dell'iscritto vengano individuate, trasformate in requisiti del servizio, comunicate al personale e soddisfatte nel quadro delle leggi vigenti e del Sistema di Gestione Integrato di cui si è dotata, coerentemente con quanto definito nel Sistema stesso.

Gli interessi degli iscritti sono monitorati anche attraverso il dialogo con gli Ordini dei Medici-Chirurghi e degli Odontoiatri i quali, grazie alla propria capacità di intercettare e condividere i bisogni degli iscritti sul territorio, rivestono un ruolo strategico ed operativo per l'Enpam.

L'Enpam si impegna a difendere e incrementare il flusso dei contributi facendo fronte e analizzando preventivamente le eventuali criticità che si dovessero prospettare.

[1] Sul sito della Fondazione è presente una sezione interamente dedicata alla trasparenza (https://www.enpam.it/fondazione-trasparente/).

3. Qualità e sicurezza dei servizi erogati e dei processi

La Fondazione si impegna ad un costante miglioramento della qualità e della sicurezza dei servizi erogati agli iscritti, perseguendo in ogni momento il più elevato livello di efficienza ed efficacia e gestendo i rischi associati alla perdita di riservatezza di integrità e di disponibilità delle informazioni trattate.
La qualità di processi e servizi è perseguita anche attraverso dotazioni strumentali tecniche ed informatiche che garantiscano un efficiente ed efficace svolgimento delle attività lavorative interne ed esterne nel rispetto dei requisiti di sicurezza.

4. Coinvolgimento e tutela dei collaboratori

L'Enpam promuove il coinvolgimento dei propri collaboratori, sia stabili che occasionali, incentivandone la formazione e la crescita professionale e impegnandosi nella creazione di un ambiente di lavoro proficuo e stimolante, basato sull'efficace scambio di conoscenze lavorative e sul comune perseguimento degli obiettivi. La Fondazione tutela inoltre la salute e la sicurezza dei propri dipendenti, ottemperando agli obblighi della vigente normativa in materia di sicurezza sul posto di lavoro.

5. Valori e principi: il Codice Etico

Il Codice Etico della Fondazione comprende – nella forma di regole e principi – il complesso di diritti, doveri e responsabilità che l'Ente espressamente assume nei confronti di ogni portatore di interesse con il quale esso interagisca nell'ambito dello svolgimento della propria attività. L'impianto di regole e principi espresso nel Codice deve ispirare l'attività di coloro che operano nella Fondazione e per la Fondazione.

6. Solidità e sostenibilità

La Fondazione riconosce la centralità e l'importanza della contribuzione, ponendo il proprio patrimonio a difesa e garanzia delle prestazioni.

La Fondazione mira altresì alla solidità del proprio patrimonio, al fine di garantire una piena sostenibilità nel medio-lungo periodo del sistema previdenziale ed assistenziale, pertanto individua la prudenza e la sicurezza quali criteri-guida per i propri investimenti finanziari e reali, anche attraverso il costante monitoraggio del rischio e

la proceduralizzazione ed il controllo delle attività relative alla gestione del Patrimonio.

La Fondazione Enpam riconosce il proprio ruolo all'interno del tessuto socio-economico nazionale, facendosi promotrice di iniziative sociali riguardanti temi quali la prevenzione ed il supporto dei corretti stili di vita. La responsabilità sociale verso la collettività si sostanzia inoltre in investimenti che mirano al sostegno, diretto ed indiretto, del Sistema Italia[2].

7. Gli obiettivi per la qualità e la sicurezza delle informazioni

La Fondazione ha definito gli obiettivi per la qualità e per la sicurezza delle informazioni sulla base della pertinenza e congruità degli stessi con gli obiettivi strategici e le potenzialità della Fondazione, configurando quindi obiettivi coerenti, raggiungibili e misurabili per verificarne l'effettivo perseguimento. Gli obiettivi per la qualità e per la sicurezza delle informazioni sono di seguito indicati:

- perseguire la soddisfazione dell'iscritto in ogni momento;
- garantire la massima sicurezza delle informazioni degli iscritti/portatori di interesse, in termini di riservatezza, disponibilità e integrità delle informazioni stesse fornendo così un servizio ad alto valore aggiunto;
- formare il personale allo svolgimento delle attività in modo da proteggere gli asset aziendali nel rispetto della vigente normativa;
- definire ruoli e responsabilità del personale coinvolto nella gestione del sistema di gestione integrato della Qualità e Sicurezza delle Informazioni;
- fornire supporto all'attività della Fondazione attraverso strumenti e mezzi tecnologicamente avanzati, mantenendo gli stessi in perfetto stato di efficienza;
- ottenere dai fornitori i livelli definiti dalla Fondazione per i servizi e i prodotti acquistati;

[2] Si tratta di: "investimenti che potenzialmente presentano una ricaduta positiva sulla crescita e sulla sostenibilità economica-sociale a medio-lungo termine del paese Italia. Tali investimenti si traducono in un sostegno indiretto per le categorie professionali dei medici e degli odontoiatri italiani attraverso il miglioramento del contesto economico-sociale in cui lavorano e delle opportunità professionali derivanti dal consolidamento/espansione della spesa sanitaria." Fonte: Manuale delle procedure operative e di controllo del patrimonio della Fondazione – PO_07 Investimenti istituzionali.

- perseguire il miglioramento continuo delle prestazioni aziendali per il Sistema di gestione per la qualità, assicurando sia la disponibilità delle risorse necessarie in termini di personale, mezzi, infrastrutture e strumenti, sia la razionalizzazione dei processi interni attraverso la stesura di procedure ottimizzate;
- monitorare le prestazioni per l'individuazione delle possibili aree di miglioramento;
- assicurare la continuità operativa ai servizi critici anche a seguito di gravi incidenti potenzialmente capaci di compromettere la sopravvivenza dell'azienda stessa;
- assicurare il rispetto degli standard qualitativi stabiliti ed attesi e, allo stesso tempo, il loro miglioramento;
- essere conformi alle disposizioni legislative, alla normativa sulla sicurezza e protezione dei dati, alla presente Politica, e a ogni altro accordo sottoscritto con le parti interessate;
- identificare in modo periodico e sistematico le minacce alla sicurezza incombenti sui dati, valutandone le esposizioni ai rischi e provvedendo ad attuare idonee azioni preventive;
- incoraggiare la diffusione della cultura e promuovere la sensibilizzazione in materia di sicurezza e protezione dei dati e delle informazioni, in particolare di riservatezza, integrità e disponibilità dei dati e delle informazioni, tra i propri dipendenti, collaboratori, partner e terze parti in merito ai loro ruoli e responsabilità in quest'ambito;
- far fronte con rapidità, efficacia e scrupolo a emergenze o incidenti che possano verificarsi nello svolgimento delle attività, collaborando anche con terze parti o Enti preposti;
- rispettare le leggi e i regolamenti in vigore nel contesto della sicurezza, e comunque attenersi a standard individuati con senso di responsabilità e consapevolezza, basati su principi scientifici e a valutazione dei rischi;
- effettuare attività di controllo e riesame sulle attività, a partire da quelle più critiche, per aggiornare i programmi di sicurezza pianificati per il raggiungimento e l'assicurazione dei requisiti di sicurezza.

La Fondazione ha predisposto, nell'ambito del proprio Sistema di gestione integrato, metodi e strumenti per il monitoraggio degli obiettivi, per la misurazione del grado di raggiungimento e per il riesame degli obiettivi stessi, nonché per la ridefinizione e/o l'individuazione di nuovi obiettivi, che sono descritti nel Manuale del Sistema di

gestione integrato per la qualità e la sicurezza delle informazioni e che trovano attuazione con le modalità prescritte nelle procedure operative di pertinenza richiamate nel Manuale stesso.

Il responsabile del Sistema di gestione integrato
Dott. Andrea Leonori

Data: 1 giugno 2023