Roma, lì 28/02/2025

La costante ricerca di nuove strategie di mercato volte a dare garanzie ai propri "stakeholders", non soltanto in termini di "qualità" dei processi finalizzati alla fornitura/erogazione "ottimale" di prodotti/servizi, ma anche sulle modalità "sicure" di trattamento delle informazioni loro riguardanti, oltre che quelli relativi alla propria struttura organizzativa, ha favorito l'Alta Direzione della **GPA GRUPPO PROGETTI AVANZATI SRL** (**GPA** od Organizzazione nel seguito del presente documento), nella decisione di implementare un **Sistema di Gestione Integrato (SGI)** coerente con gli schemi **ISO 9001:2015** e **ISO/IEC 27001:2022** come unico strumento organizzativo che integra ed armonizza gli aspetti significativi dei singoli sistemi di gestione, favorendone in ultima analisi il miglioramento continuo di ognuno di essi.

Con tale **SGI** la **GPA** si prefigge:

- il rispetto puntuale dei requisiti delle norme di riferimento: **UNI EN ISO 9001:2015** per la gestione "in qualità" dei propri processi e **ISO/IEC 27001:2022** per assicurare la sicurezza delle informazioni trattate;
- di razionalizzare i processi aziendali, con conseguente ottimizzazione dell'utilizzo delle risorse umane e tecniche anche con un "focus" particolare all'impegno a minimizzare il proprio impatto in materia di cambiamenti climatici;
- di orientare le proprie decisioni, i processi e i progetti soppesando contestualmente i rischi e/o valutando il conseguimento delle opportunità;
- di individuare ruoli e responsabilità specifiche all'interno dell'Organizzazione ovvero determinare le risorse necessarie alla pianificazione e alla realizzazione dei programmi finalizzati al raggiungimento degli obiettivi;
- di assicurare il costante aggiornamento tecnico e professionale delle risorse umane dell'Organizzazione;
- di promuovere la sensibilizzazione, il coinvolgimento e la consapevolezza delle risorse umane dell'Organizzazione sull'applicazione del SGI stesso ovvero della documentazione e delle registrazioni previste;
- di sviluppare, mantenere e migliorare l'infrastruttura tecnologica per supportare i processi aziendali, preferendo strutture a basso impatto climatico;
- di assicurare il pieno rispetto delle norme, dei regolamenti e delle leggi applicabili;
- di assicurare il rispetto del proprio Codice Etico promovendo comportamenti basati sui criteri di correttezza, lealtà ed integrità morale.

In particolare, con riferimento ai requisiti dello schema **ISO 9001:2015** tutta la **GPA** è impegnata in programmi che, attraverso la stretta collaborazione delle funzioni aziendali, permettano il raggiungimento dei seguenti obiettivi:

- cooperare con i Clienti al fine di ottenere la loro piena soddisfazione e conseguentemente accrescere il valore dei loro investimenti;
- mantenere un adeguato livello delle prestazioni, in particolare garantendo la qualità dei prodotti rilasciati ovvero l'efficienza e la continuità dei servizi forniti nel rispetto dei requisiti e degli SLA richiesti;
- rispettare i tempi di esecuzione ed ottimizzare ove possibile il rapporto costo/qualità dei prodotti/servizi forniti;
- allineare le modalità di progettazione e di sviluppo dei sistemi software nonché l'erogazione dei servizi IT coerentemente ai modelli aggiornati di Best Practice internazionalmente riconosciuti applicabili ai contratti ICT;

- orientare per quanto possibile la ricerca e lo sviluppo di soluzioni e servizi dell'Information Technology, con particolare riguardo alle possibilità offerte dai sistemi open source e dalle tecnologie innovative, accrescendo contestualmente le proprie competenze nell'ambito della consulenza specialistica;

Con riferimento ai requisiti dello schema **ISO/IEC 27001:2022** la **GPA** si prefigge inoltre di proteggere da tutte le minacce, interne o esterne, intenzionali o accidentali, il proprio patrimonio informativo aziendale, ivi comprese le informazioni e i dati relativi ai propri "stakeholders", acquisiti direttamente o indirettamente anche nell'ambito dell'erogazione dei propri servizi. Contestualmente si prefigge di mantenere e dimostrare la correttezza del trattamento delle informazioni acquisite e di dare evidenza inoltre, che i servizi erogati non causino direttamente o indirettamente un aumento dei rischi in termini di perdita di **riservatezza**, **integrità** e **disponibilità** (**R.I.D.**) delle informazioni stesse, comprese nel perimetro definito dal SGI.

GPA pianifica e verifica periodicamente, specifici obiettivi per la sicurezza delle informazioni finalizzati in particolare:

- a garantire le prescrizioni previste dalla normativa vigente con particolare riferimento al regolamento Europeo UE 2016/679-GDPR in materia di protezione dei dati personali;
- a garantire la continuità del business dell'organizzazione e soddisfare contestualmente gli interessi in termini di sicurezza delle informazioni dei propri "stakeholders";
- a cooperare con i Clienti e con i Fornitori al fine di accrescere il livello di sicurezza delle informazioni trattate attraverso prodotti e servizi;
- alla costante ricerca di sistemi tecnologici innovativi che garantiscano il miglioramento della sicurezza delle informazioni;

Per il perseguimento di tali finalità, la **GPA** si impegna affinché:

- le informazioni siano protette da accessi non autorizzati nel rispetto della riservatezza e siano disponibili agli utenti autorizzati quando necessario;
- sia garantita l'integrità delle informazioni mediante interventi idonei atti a contrastare il verificarsi di modifiche non autorizzate compresi gli errori umani, o il danneggiamento dei supporti fisici contenenti le stesse;
- vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- venga regolarmente monitorato l'eventuale evoluzione delle minacce e delle vulnerabilità associate, ovvero sia garantito il mantenimento dei rischi al livello ritenuto accettabile attraverso l'implementazione di idonee contromisure;
- tutte le violazioni della sicurezza delle informazioni e i possibili punti di debolezza vengano registrati e riferiti a chi di dovere ed esaminati;
- venga attentamente monitorato il livello di "compliance" al quadro normativo nazionale/europeo ovvero agli eventuali vincoli di legge;
- il proprio personale sia adeguatamente formato/informato sui temi della sicurezza delle informazioni e sull'evoluzione delle minacce informatiche.

Per il conseguimento dei sopradetti obiettivi, l'Alta Direzione della **GPA** si impegna a far sì che la presente Politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche dagli "stakeholder" esterni (Clienti, collaboratori esterni, consulenti, fornitori, etc.), ovvero da tutte quelle figure che siano in qualsiasi modo coinvolte con i processi e le informazioni che rientrano nel campo di applicazione del Sistema di Gestione Integrato della **GPA**.

L'Alta Direzione della **GPA,** infine, si impegna a riesaminare regolarmente la presente Politica ovvero ad introdurre le necessarie modifiche atte a garantire che la stessa permanga idonea all'attività e alla capacità della **GPA** di soddisfare i requisiti e le aspettative delle parti interessate ritenute rilevanti.

Il Presidente del CdA

(Giuseppe PETRINI)