

	Politica della Qualità e della Sicurezza delle Informazioni	DOC002 - Ver. 1.0 del 17-02-2025
		Autore: RSGQSI Approvato da: Direzione Tipo Documento: Pubblico

La Direzione di Ambercom ha adottato un Sistema di Gestione della Qualità e della Sicurezza delle Informazioni (SGQSI) in conformità alle norme ISO 9001:2015 e ISO 27001:2022 integrata dai controlli previsti dalle linee guida ISO 27017:2015 e ISO 27018:2019. Ambercom è una realtà aziendale nata nel 2021 da una scissione societaria per operare in maniera più focalizzata nel settore dello sviluppo di applicativi proprietari in ambito energetico e promuovere progetti di sostenibilità con applicativi provenienti dal Property & Facility management in un'ottica ESG.

L'erogazione di servizi di qualità e la sicurezza e la salvaguardia del patrimonio informativo, costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di AMBERCOM. I requisiti per la qualità e la sicurezza delle informazioni sono coerenti con gli obiettivi dell'Organizzazione e il SGQSI rappresenta lo strumento che consente l'individuazione di corrette best practice e/o best in class per il miglioramento costante della qualità aziendale, la condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni a livelli accettabili. In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di disponibilità, integrità e riservatezza delle informazioni attraverso l'adozione di un formale "Sistema di Gestione Qualità e della Sicurezza delle Informazioni" (SGQSI) in linea con i requisiti attesi dagli stakeholder di AMBERCOM. In particolare, il SGQSI è applicato a:

"Progettazione, sviluppo ed erogazione di software On Premise ed in modalità SAAS, sia per aziende private che per la Pubblica Amministrazione come da Statement Of Applicability vers. 1.0 del 17-02-2025, integrato dai controlli previsti dalle linee guida ISO 27017:2015 e della ISO 27018:2019. Erogazione dei connessi servizi di supporto ed assistenza tecnica."

Obiettivi primari dell'Organizzazione, sostenuti dall'impegno della Direzione sono:

- l'ottenimento della completa soddisfazione delle esigenze, delle aspettative del Cliente e del mercato;
- il conseguimento e il mantenimento di un'ottima reputazione in fatto di Qualità dei propri servizi;
- ottenere un elevato grado di soddisfazione della Clientela anche grazie alla pianificazione delle attività, la strutturazione per processi, l'abitudine a seguire scrupolosamente le procedure aziendali, le continue ed attente attività di verifica;
- fornire servizi e strumenti tattici alle aziende per consentire loro di essere più competitive, organizzando i consumi energetici specifici per centri di costo in funzione degli obiettivi aziendali e migliorando in modo continuo la gestione dei propri dati in un'ottica di efficientamento del tempo/uomo dedicato alle attività di rendicontazione;
- proporre ai clienti soluzioni personalizzate, flessibili e configurabili in modo da rispecchiarne le esigenze e l'immagine aziendale, garantendo i requisiti attesi dal punto di vista della qualità;
- offrire strumenti informatici stabili, affidabili e all'avanguardia utilizzando le più moderne tecnologie web;
- fornire assistenza rapida a costi adeguati utilizzando strumenti per il controllo remoto, evidenziando un impegno continuativo sul piano formativo ed affiancamento all'uso per verifiche di coerenza, dando così un grande valore aggiunto alle attività ordinarie legate all'applicativo;
- garantire nell'implementazione del progetto la massima trasparenza con i clienti, condividendo le informazioni ed i dati riguardanti le attività;
- ricercare l'eccellenza del prodotto fornito e del servizio erogato;
- migliorare con continuità l'efficacia del SGQSI;
- promuovere un approccio sistemico ai processi aziendali attraverso l'adozione di strumenti e metodologie standard;
- condividere a tutti i livelli aziendali la cultura per la qualità e il rispetto delle regole;
- promuovere l'approccio del *risk-based thinking* all'interno dell'organizzazione;
- realizzare, ove possibile i progetti con una soluzione standard, semplice e con tempi di implementazione ridotti integrando dati da svariate fonti e rendendo il nostro applicativo l'unica porta di ingresso per le attività di monitoraggio energetico;
- creare un'azienda a misura d'uomo: sviluppare una squadra motivata, competente, soddisfatta ed orgogliosa;
- dimostrare ai propri stakeholders di erogare servizi di qualità che seguano processi definiti e volti al miglioramento continuo;
- dimostrare ai clienti la propria capacità di fornire con regolarità servizi sicuri, massimizzando gli obiettivi di business;

- minimizzare il rischio di perdita e/o indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua e adeguata analisi dei rischi che esaminano costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- promuovere la collaborazione, comprensione e consapevolezza del SGQSI da parte dei fornitori strategici;
- conformarsi ai principi e ai controlli stabiliti dalla ISO 9001, ISO 27001, ISO 27017 e ISO 27018 o altre norme/regolamenti che disciplinano le attività di business in cui opera l'azienda, tra i quali, in particolare, le regolamentazioni inerenti alla Privacy e la sicurezza dei dati personali (GDPR).

In particolare, per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO 27017, la direzione si impegna ad adottare requisiti di sicurezza che prendano in considerazione i rischi derivanti dal personale interno, la gestione sicura del multi-tenancy (condivisione dell'infrastruttura), l'accesso agli asset in cloud dei clienti da parte del personale del service provider, il controllo degli accessi (in particolare degli amministratori), le comunicazioni ai clienti in occasione di cambiamenti dell'infrastruttura, la sicurezza dei sistemi di virtualizzazione, la protezione e l'accesso dei dati dei clienti in ambiente cloud, la gestione del ciclo di vita degli account cloud dei clienti, la comunicazione degli incidenti e dei data breach e linee guida per la condivisione delle informazioni a supporto delle attività di investigazione e forensi nonché la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud.

Inoltre, l'azienda è costantemente impegnata nella protezione dei dati personali degli interessati che gestisce, con particolare riferimento a quelli dei propri clienti. Rispetto a questi ultimi l'azienda, ai sensi della ISO 27018 e in accordo con la legislazione privacy vigente (GDPR), agisce come "Data Processor" ovvero come "Responsabile del Trattamento" ex art. 28 del GDPR, dichiarando questo status e i relativi obblighi che ne discendono nei contratti con i clienti. Tali obblighi sono riportati anche nelle nomine a responsabile dei fornitori utilizzati.

Tutta l'azienda ed i suoi partner sono coinvolti nella segnalazione di eventuali non conformità rispetto ai risultati attesi sulla qualità dei servizi o nella gestione degli aspetti di sicurezza delle informazioni, nella segnalazione e gestione di reclami da parte dei clienti e/o di incidenti riscontrati sotto il profilo della sicurezza delle informazioni, nonché di qualsiasi debolezza identificata nel SGQSI e si impegnano nel supportare l'implementazione, la messa in opera, il riesame periodico ed il miglioramento continuo del SGQSI.

La presente Politica viene concretamente applicata attraverso:

- la definizione di specifici obiettivi e indicatori misurabili;
- la disponibilità delle risorse necessarie;
- il comportamento partecipativo di tutto il personale dell'azienda.

La Politica viene periodicamente verificata, nel corso del riesame di direzione, nella sua adeguatezza, alla luce di eventuali cambiamenti di circostanze e conoscenze. Gli obiettivi per la qualità e la sicurezza delle informazioni sono definiti annualmente durante il riesame di Direzione di Ambercom e comunicati a tutti i livelli aziendali.

Per realizzare quanto indicato sopra, il nostro agire quotidiano mette al centro:

- l'attenzione per il Lavoratore, quale principale risorsa di valore per l'Organizzazione;
- l'attenzione per la Professionalità, quale strumento imprescindibile del proprio agire quotidiano;
- l'attenzione per la Serietà e Trasparenza, quali guide del proprio operare;
- l'attenzione per la Qualità, quale metodo primario per la realizzazione dei nostri servizi;
- l'attenzione per la Sicurezza, quale condizione necessaria per operare sul mercato.

Il vertice aziendale si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica, con il fine ultimo del miglioramento continuo della qualità del suo operato e della sicurezza delle informazioni nell'erogazione dei suoi servizi.

L'Amministratore Unico

Andrea Pavesi

