All. 3

Politica della Qualità e della Sicurezza delle Informazioni

Indice

1 Proprietà del documento

Proprietà	Descrizione
Titolo	Politica della Qualità e della Sicurezza delle Informazioni
Codifica	All. 3
Classificazione	Pubblico
Tipo	Politica
Nome del file	All. 3 Politica della Qualità e della Sicurezza delle Informazioni
Proprietà	Sababa Security SpA | Sistemi di Gestione
Autore	Alessio Aceti
Data di creazione	02/05/2022
Modificato da	
Versione	1
Data	02/05/2022
Stato	Rilasciato
Lingua	Italiano

1.1 Storia del documento

Versione	Data	Descrizione	Autore	Stato
1	02/05/2022	Prima versione	Alessio Aceti	Rilasciato

2 Politiche aziendali

Sababa Security attua una politica per la qualità focalizzata sull'ottenere la soddisfazione, la fiducia e la fidelizzazione del Cliente e sulla conformità alle normative e leggi cogenti, al fine di conseguire e mantenere i seguenti obiettivi:

- essere un punto di riferimento per i Clienti per l'affidabilità dei prodotti forniti e dei servizi erogati, col rispetto dei livelli di servizio e dei tempi di rilascio concordati;
- assicurare l'eccellenza nella relazione;
- garantire la soddisfazione delle esigenze espresse ed implicite del Cliente e dei requisiti cogenti.

L'impegno aziendale nel perseguire tali obiettivi è dimostrato dall'adozione, sistematica attuazione, verifica e miglioramento continuo del Sistema di Gestione per la Qualità conforme alla norma UNI EN ISO 9001:2015.

Analogamente un altro obiettivo primario perseguito da Sababa Security consiste nel garantire la sicurezza e protezione delle informazioni e dei dati affidati dalla Clientela, come pure la protezione e affidabilità delle strutture tecnologiche, fisiche, logiche ed organizzative, responsabili della gestione di dati/informazioni.

A questo scopo Sababa Security ha deciso di stabilire, attuare, mantenere e migliorare in modo continuo un Sistema di Gestione per la Sicurezza delle Informazioni che sia contestualmente conforme alla norma UNI CEI EN ISO/IEC 27001:2017, al Regolamento Europeo 2016/679, alla normativa italiana in materia di privacy e che consenta di perseguire i seguenti macro obiettivi:

- definire gli opportuni livelli di riservatezza delle informazioni e garantirli attraverso processi e controlli che consentono di raggiungere i risultati attesi e concordati con la Clientela;
- assicurare l'integrità delle informazioni gestite per conto della Clientela, attraverso opportuni processi e controlli;
- adottare, in accordo con la Clientela, i processi e i controlli che consentano di garantire la disponibilità delle informazioni da essa attesa;
- valutare costantemente i rischi per la sicurezza delle informazioni presenti nei processi di erogazioni dei servizi alla Clientela e adottare le conseguenti azioni di trattamento;
- mettere in atto le azioni più opportune per consentire che le risorse impegnate abbiano la competenza e la consapevolezza sulla sicurezza delle informazioni adeguate.

3 Obiettivi

Gli obiettivi di dettaglio perseguiti sono:

1. mantenere un sistema di gestione della qualità costantemente aggiornato e applicato in conformità alla norma UNI EN ISO 9001:2015;
2. mantenere un sistema di gestione della sicurezza delle informazioni aggiornato e conforme alla norma UNI CEI EN ISO/IEC 27001:2017, ai requisiti cogenti e contrattuali applicabili alla sicurezza delle informazioni ed al rispetto della privacy;
3. assicurare l'accesso alle informazioni alle sole persone autorizzate (interne o esterne), anche tramite un'accurata gestione delle credenziali sui sistemi informativi adottati;
4. assicurare la riservatezza delle informazioni, anche mediante crittografia;
5. assicurare l'integrità delle informazioni;
6. attuare il "Piano di backup" e mantenere, validare e testare periodicamente il "Piano di continuità operativa del business e disaster recovery";
7. garantire la protezione degli asset aziendali;
8. attuare e ripetere ciclicamente l'identificazione, la valutazione e il trattamento dei rischi al fine di attuare i necessari trattamenti per la loro eliminazione o mitigazione;
9. garantire la presenza di adeguate risorse (hardware e software) a supporto della qualità dei servizi e prodotti erogati alla Clientela e della sicurezza delle informazioni;
10. garantire una formazione continua volta ad aumentare il livello di competenza del Personale negli ambiti della relazione con la Clientela, della gestione dei sistemi, reti e applicazioni critiche, della conoscenza e rispetto delle migliore pratiche e misure finalizzate alla sicurezza delle informazioni.