

POLITICA DELLA QUALITA' E DELLA SICUREZZA 2024

La Politica per la Qualità e Sicurezza documenta quelli che sono gli obiettivi ed impegni in funzione delle strategie aziendali verso i clienti ed i dipendenti dell'azienda stessa, affinché siano attuate, mantenute e migliorate le prestazioni del Sistema di Gestione Integrato ISO9001-ISO27001.

Scenario ritiene determinante la partecipazione di tutto l'organico alla completa attuazione del Sistema di Gestione Integrato, in modo da raggiungere il consolidamento sul mercato da raggiungere attraverso la soddisfazione per i servizi erogati e le garanzie fornite ai propri clienti.

Per ricercare e mantenere una posizione di rilievo nel mercato e raggiungere la soddisfazione e la fidelizzazione del cliente, Scenario si impegna costantemente nel:

- Operare una selezione sistematica di nuovi prodotti di alto livello tecnologico,
- Adottare strumenti tecnici più innovativi ed affidabili, rendendo più efficiente l'organizzazione dei propri servizi e più sicuri e controllati i processi per integrare le attività del cliente.
- Adottare delle policy tecniche per la gestione e per la sicurezza delle informazioni ovvero la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.

Per adempiere alla propria missione, Scenario intende:

- Promuovere la partecipazione attiva dei collaboratori e dei dipendenti al fine di rendere più efficienti i servizi erogati;
- Diffondere nell'organizzazione cultura e metodologie appropriate in modo che chiunque vi lavori sia costantemente in grado di erogare il miglior servizio atteso al cliente;
- Formare il personale affinché possa sviluppare non solo le proprie competenze tecniche ma anche quelle organizzative;
- Consolidare il rapporto con i vendors e distributori riconosciuti dal mercato al fine di assicurare ai clienti prodotti di maggior valore, sicuri, affidabili, di alto livello tecnologico;
- Favorire proficue partnership in modo da poter essere parte attiva nella definizione delle prestazioni e delle caratteristiche del prodotto, ed a fornire il supporto necessario per la comprensione e definizione dei requisiti del Cliente e dei requisiti tecnici pertinenti il prodotto;
- Mantenere e consolidare un Sistema di Gestione Integrato quale strumento per realizzare e monitorare gli obiettivi, rispettare gli impegni assunti, promuovere il miglioramento continuo dei processi aziendali, garantire il rispetto dei requisiti cogenti per i prodotti ed i servizi correlati;
- Promulgare procedure che garantiscano il mantenimento della riservatezza, integrità, disponibilità, autenticità delle informazioni e dei dati presenti e gestiti nell'ambito delle attività.
- Sensibilizzare il personale nel corretto uso delle informazioni e dei mezzi di comunicazione al fine di garantire la puntualità delle trasmissioni e la capacità di dimostrare che un'azione o un evento hanno avuto luogo (non ripudio) evitando possibili contestazioni.
- Incoraggiare la crescita professionale e garantire un ambiente di lavoro sicuro che tuteli la sicurezza e la riservatezza delle informazioni.

Nella pratica Scenario ha identificato i soggetti coinvolti nella gestione delle informazioni definendo con precisione i ruoli e le responsabilità di ciascuno e inserendo a sistema i documenti (procedure) che le descrivono nel dettaglio. Sono altresì definite le procedure per identificare, trattare, impedire eventuali incidenti relativi alla sicurezza delle informazioni e consentire di migliorare progressivamente il sistema di trattamento.

SCENARIO

Gli obiettivi principali dell'Information Security Policy sono i seguenti:

- Garantire la conformità con leggi, regolamenti e linee guida.
- Istituire controlli per la protezione dei sistemi informativi e delle informazioni di Scenario contro il furto, gli abusi e altre forme di danneggiamento e perdita.
- Motivare gli amministratori e i dipendenti a mantenere la responsabilità, la proprietà e la conoscenza della sicurezza delle informazioni, al fine di minimizzare il rischio di incidenti di sicurezza.
- Assicurare che Scenario sia in grado di continuare i propri servizi anche in caso di gravi incidenti di sicurezza.
- Assicurare la protezione dei dati personali (privacy).
- Assicurare la disponibilità e l'affidabilità delle infrastrutture di rete e dei servizi forniti e gestiti da Scenario.
- Rispettare i metodi degli standard internazionali per la sicurezza delle informazioni, ad esempio, ISO/IEC 27001.
- Assicurarsi che i fornitori esterni di servizi siano conformi ai bisogni e le esigenze di sicurezza delle informazioni di Scenario.
- Assicurare la flessibilità e un livello accettabile di sicurezza per l'accesso ai sistemi di informazione dall'esterno

La strategia adottata prevede le seguenti attività principali:

- Risk Assessment
- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione della Business Continuity e del Disaster Recovery
- Monitoraggio, tracciamento e verifiche tecniche
- Introduzione di nuovi sistemi e servizi
- Operation Management
- Rispetto della normativa