



POLITICA DELLA QUALITÀ
E SICUREZZA DELLE INFORMAZIONI

Politica della Qualità e Sicurezza delle Informazioni

La nostra azienda, nelle attività di “progettazione e realizzazione di servizi nell'ambito system integration e security” si impegna a perseguire e garantire nel tempo, oltre il rispetto della normativa cogente, la sempre maggiore soddisfazione del cliente e delle altre parti interessate migliorando sempre più il servizio erogato, fornendo servizi globali e soluzioni alla gestione di sistemi e infrastrutture.

Il miglioramento richiede il coinvolgimento e la partecipazione di tutti coloro che sono ritenuti fattori rilevanti interni ed esterni per il nostro contesto e si fonda sui seguenti punti:

- Qualità è far bene le cose giuste sin dalla prima volta. Questo comporta un maggiore impegno iniziale, ma una riduzione delle correzioni nel tempo.
- La Direzione, a partire dalle esigenze del Cliente e da quelle del mercato, definisce annualmente un Piano di Miglioramento aziendale e obiettivi per i processi ritenuti significativi. Ciascun Responsabile di Funzione deve, sulla base di quanto indicato dalla Direzione, portare avanti i piani d'azione definiti per raggiungere i traguardi fissati.
- Il coinvolgimento più ampio e frequente di tutte le risorse interne ed esterne è prerequisito fondamentale per il continuo miglioramento dei processi, delle opere e del servizio.
- I nostri Fornitori devono essere coinvolti nel nostro programma di miglioramento. Essi sono infatti un anello della nostra catena produttiva.



Il successo dell'Azienda passa attraverso il miglioramento professionale e culturale delle singole risorse. È pertanto prevista l'individuazione di un preciso e coerente Piano di Formazione volto all'effettiva crescita di tutte le risorse.

Per garantire questo "impegno", la Direzione ha deciso di introdurre e mantenere un sistema di gestione che risponda alle norme internazionali UNI EN ISO 9001:2015 ("Sistemi di gestione per la qualità"), UNI CEI ISO/IEC 27001:2018 ("Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni"), ISO/IEC 27017:2015 ("Linea guida per i controlli di sicurezza delle informazioni per i servizi in Cloud") e ISO/IEC 27018:2019 ("Linea guida per la protezione dei dati personali trattati nei servizi Cloud pubblici"), a partire dalla determinazione dei fattori interni ed esterni ritenuti rilevanti per i nostri indirizzi strategici, pensando ed agendo secondo un sistema di gestione del rischio (Risk Based Thinking) basato sulla capacità di assumere decisioni e intraprendere azioni non in modo meccanico e acritico, pur nel rispetto delle procedure previste, ma come effetto di una valutazione razionale delle possibili conseguenze, positive o negative, delle proprie scelte, per garantire la conformità ai requisiti contrattuali, tecnici, qualitativi, di sicurezza delle informazioni, inclusi quelli cogenti nei confronti di tutte le parti interessate.

La Direzione quindi, con il coinvolgimento e la partecipazione delle risorse interne ed esterne interessate, si impegna a:
Garantire la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di sicurezza.

- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema di gestione qualità e sicurezza delle informazioni siano tempestivamente riconosciuti e corretta-



- mente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da parte di personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- Garantire la conformità ai requisiti di legge ed il rispetto degli impegni stabiliti nei contratti con terze parti.
- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- Garantire la Business Continuity aziendale e il Disaster Recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
- Garantire che i cambiamenti attuati siano migliorativi del servizio offerto e del livello di sicurezza.
- Garantire che eventuali cambiamenti che hanno impatto sul cliente siano adeguatamente comunicati.
- Garantire un elevato livello di competenza e consapevolezza attraverso l'attuazione di appositi piani formativi.
- Garantire che la politica, rappresentando il quadro di riferimento per la definizione di obiettivi e traguardi di miglioramento specifici, sia periodicamente riesaminata per verificarne la continua adeguatezza agli scopi aziendali, diffusa, compresa e attuata dal personale interno e da collaboratori esterni che lavorano per la nostra organizzazione o per conto di essa e sia disponibile a clienti e altre parti interessate attraverso pubblicazione sul sito web.

La Direzione


