ATHENA SRL
Cap.Soc. € 200.000 i.v.
Sassari: P.Niedda Nord str.28
Tel. 079 – 2638500
Fax 079 – 2638528
Cagliari: Via dell'Artigianato 13
Tel. 070 –2110104
Fax 070 –2110318
www.athenasardegna.it

POLITICA PER LA GESTIONE DELLA QUALITÀ E DELLA SICUREZZA DELLE INFORMAZIONI

EN-ISO 9001:2018 – ISO/IEC 27001:2013

Raggiungere l'eccellenza è l'impegno della nostra Società.

Per rendere concreta quest'asserzione abbiamo riassunto i principi guida del nostro comportamento che devono sempre ispirarci a prescindere dalla strategicità del ruolo.

La formazione del personale deve essere improntata a questi principi.

Tutto ciò che facciamo trae origine ed è finalizzato al cliente.

Noi vogliamo fornire il servizio che meglio si adatta alle esigenze dei clienti con l'impegno di soddisfare tutti i requisiti applicabili, sia quelli espliciti che impliciti che cogenti.

Noi vogliamo assicurare che i bisogni reali dei nostri clienti siano capiti e portati a conoscenza di tutta l'organizzazione.

Noi vogliamo assicurare un ambiente di lavoro che consenta di raggiungere i nostri obiettivi.

Vogliamo approfondire la conoscenza dell'ambiente esterno, cogliere i cambiamenti ed adeguarci all'evoluzione della tecnologia e del mercato.

Vogliamo coinvolgere il personale con continuità; renderlo partecipe degli obiettivi e dei risultati aziendali.

Vogliamo operare secondo un Sistema Qualità costruito secondo i suggerimenti e l'esperienza di norme codificate.

Vogliamo operare secondo uno schema per processi per definire meglio la nostra attività e per misurarne, attraverso gli indicatori, il miglioramento continuo.

Vogliamo uniformare e standardizzare il nostro operato con il sistema informatico gestionale interno; ciò consente la condivisione delle linee di azione e l'immediata rilevazione di situazioni critiche.

Vogliamo basare le nostre azioni di miglioramento su dati di fatto concreti.

Vogliamo valutare assieme il miglioramento delle nostre prestazioni.

Vogliamo individuare e favorire i fornitori con i quali si possono sviluppare relazioni di reciproco vantaggio.

Questi orientamenti della direzione sono riassunti nella frase esposta negli uffici:

La qualità delle nostre prestazioni consiste nel rispetto degli impegni assunti e si misura con la soddisfazione del cliente.

Nella parte del Sistema di Gestione Integrato che riguarda la Sicurezza delle Informazioni (che è il Sistema di Gestione della Sicurezza delle Informazioni – SGSI), attribuiamo importanza strategica al trattamento delle informazioni stesse, per concretizzare la volontà di garantire la riservatezza, l'integrità e la disponibilità dei dati (il cosiddetto paradigma "RID"), in accordo ai principi della UNI CEI ISO/IEC 27001:2013.

I principi cardine del SGSI sono quelli atti ad assicurare:

- la riservatezza del patrimonio informativo gestito, per cui l'informazione non è resa disponibile o comunicata ad individui e/o entità non autorizzati;
- l'integrità del patrimonio informativo gestito, e cioè che i dati e le informazioni siano protetti da modifiche non autorizzate;
- la disponibilità del patrimonio informativo gestito, per cui l'informazione deve essere disponibile, accessibile e utilizzabile quando necessario (pur sempre rispondendo al criterio delle riservatezza di cui sopra);
- l'ottemperanza ai requisiti cogenti, normativi e contrattuali;

- la redazione di piani per la continuità dell'attività, e che tali piani siano il più possibile tenuti aggiornati e controllati;
- l'adeguata formazione del personale in tema di sicurezza delle informazioni;
- la corretta gestione di tutte le violazioni alla sicurezza delle informazioni e dei possibili punti deboli, al fine di una corretta rilevazione ed indagine, con conseguente miglioramento del Sistema.

Gli obiettivi del SGSI possono pertanto essere sintetizzati in:

- individuare una adeguata metodologia di valutazione del rischio correlato al business, tesa ad identificare il valore del patrimonio informativo da proteggere, la sua vulnerabilità e le possibili minacce che possano insidiarlo;
- stabilire quale è il livello di rischio accettabile;
- definire le linee operative per una architettura di sicurezza, intesa come l'insieme coordinato di regole, funzioni, strumenti, oggetti e controlli, che garantiscano in ogni ambito gestito (struttura, ambiente informatico, singolo elaboratore) il rispetto degli standard definiti dall'azienda;
- rendere effettive le linee operative di cui al punto precedente;
- controllare, cogliendo ogni spunto di miglioramento, il sistema attuato;
- assicurare che siano identificati e continuativamente aggiornati tutti i requisiti cogenti e regolamentari applicabili;
- assicurare che i requisiti siano utilizzati come "dati di ingresso ai processi" e che ne sia riscontrata la conformità nell'ambito del monitoraggio sui "dati di uscita dai processi", approccio questo da utilizzarsi in particolare nelle attività di audit interno;
- assicurare la conformità del Sistema ai requisiti cogenti.

ATHENA ha definito i criteri di valutazione del rischio della sicurezza delle informazioni considerando in particolare il valore strategico che ha per l'azienda l'applicazione del SGSI, le aspettative e le percezioni delle parti in causa (stakeholders) e i possibili danni all'immagine che potrebbero conseguire da una non corretta gestione di tale importante ambito.

L'elenco degli aspetti cogenti e normativi è riportato nel documento "Banca Dati Normativa". I criteri per la ponderazione del rischio sulla base dell'impatto e della probabilità di accadimento sono riportati nel documento "Identificazione e Valutazione dei Rischi".

Siamo consci che la sicurezza informatica, non consiste semplicemente in un prodotto/sistema tecnologico da acquistare, ma è un processo culturale complesso, che deve coinvolgere tutte le risorse umane ed organizzative aziendali.

Per tale ragione la Direzione autorizza tutte le attività volte a condurre ed implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sulla base della presente politica e a fronte dei requisiti della norma ISO 27001:2013.

Tutto il personale di **ATHENA** e i collaboratori che siano in qualche modo coinvolti con il trattamento di informazioni che rientrano nel campo di applicazione del SGSI sono responsabili dell'attuazione della presente politica, con il supporto della Direzione che ha approvato la politica stessa.

Il Responsabile del Sistema di Gestione per la Qualità e per la Sicurezza delle Informazioni facilita l'attuazione della presente politica attraverso lo sviluppo di norme e procedure appropriate.

Tutto il personale e i collaboratori devono seguire le procedure stabilite dalla Direzione per la politica della sicurezza delle informazioni.

Tutto il personale, in base alle proprie conoscenze, ha la responsabilità di riferire al Responsabile della Sicurezza delle Informazioni qualsiasi punto debole individuato.

Qualsiasi azione, che in modo intenzionale o riconducibile a negligenza, provocherà un danno all'Azienda, potrà essere perseguita nelle opportune sedi.

L'Amministratore

Sassari, 2 gennaio 2021