Norma di riferimento*: ISO/IEC 27001:2017*

Politica per la sicurezza delle informazioni

Motivazione

ITEC Tecnologie e Impianti Spa è una società che svolge attività di progettazione, installazione e manutenzione di impianti di videosorveglianza, antintrusione, rilevazione e spegnimento incendi. Data la natura delle proprie attività, considera la sicurezza delle informazioni un importante fattore per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica facilmente trasformabile in vantaggiocompetitivo.

ITEC pone particolare attenzione ai temi riguardanti la sicurezza delle informazioni gestite, che devono essere ritenuti un bene primario dell'azienda.

Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a tutte le attività di Gestione in sicurezza delle informazioni interne e delle informazioni di proprietà del cliente in tutti i servizi di: videosorveglianza e installazione / manutenzione anti-intrusione e attività di manutenzione dei sistemi antincendio.

Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni riservate, gli uffici operano secondo normative di sicurezza internazionalmente riconosciute.

Per questo motivo si intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello affidato dai propri Clienti.

Su tali basi ITEC ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma internazionale ISO/IEC 27001:2017.

Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di ITEC è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito tutte le attività di progettazione, costruzione e manutenzione di sistemi di videosorveglianza, anti-intrusione e attività di manutenzione dei sistemi antincendio, attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione per la Sicurezza per le Informazioni definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **RISERVATEZZA**: la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati;
- **INTEGRITÀ**: la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico, che sia stata modificata in modo legittimo da soggetti autorizzati e che ne rimanga traccia;
- **DISPONIBILITÀ**: la garanzia di reperibilità dell'informazione in relazione alle esigenze di utenti e clienti ed in relazione al rispetto delle norme;

Inoltre con la presente politica ITEC intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza.

Contenuto della politica

Il SGSI si applica a tutte le attività di Gestione in sicurezza delle informazioni interne e delle informazioni di proprietà del cliente in tutti i servizi di: videosorveglianza e installazione / manutenzione anti-intrusione e attività di manutenzione dei sistemi antincendio.

Tutte le informazioni, che vengono create o utilizzate dall'Azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile, e debbono essere prontamente disponibili per gli usi consentiti.

È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Il sistema prevede – in conformità alla norma ISO/IEC 27001:2017 – che il Responsabile per la Sicurezza delle Informazioni svolga periodicamente un'analisi dei rischi che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti; l'analisi dei rischi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate.

La Direzione condivide con il Responsabile della Sicurezza delle Informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della metodologia la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito all'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti accogliendo la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

Tale analisi sarà ponderata anche rispetto al valore di business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.

Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

Responsabilità

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa politica e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Il **responsabile della sicurezza delle informazioni** si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

- emanare tutte le procedure e politiche necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- adottare criteri e metodologie per l'analisi e la gestione del rischio;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività aziendali ;
- pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;

- verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con ITEC devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

Applicabilità

La presente politica si applica indistintamente a tutto il personale dell'Azienda così come per i Consulenti, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda.

ITEC consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

Scopo del SGSI

Il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) si applica a tutte le attività di Gestione in sicurezza delle informazioni interne e delle informazioni di proprietà del cliente in tutti i servizi di: videosorveglianza e installazione / manutenzione anti-intrusione e attività di manutenzione dei sistemi antincendio.

Riesame

ITEC verificherà periodicamente l'efficacia e l'efficienza del Sistema di Governo per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Novi Ligure, 07/01/2019

Approvato dalla Direzione

Amministratore Unico

Alessandra Torrielli