Sezione di controllo delle versioni

Vers.	Data	Descrizione
00	30/04/2021	Prima emissione
01	21/05/2025	Aggiornamento ed integrazione con nuove norme

Classificazione informazioni
Riservate x Interne Pubbliche

Sommario

Classificazione informazioni
Riservate x Interne Pubbliche

1. Premessa

A.I.C.E. Consulting S.r.l. è una società che fornisce servizi che includono la diagnostica strutturale, il monitoraggio, la progettazione, la direzione dei lavori, il collaudo e le altre prestazioni tecniche in genere, aventi per oggetto prevalente, ma non esclusivo, le costruzioni civili ed industriali con i relativi impianti, le infrastrutture di viabilità e trasporto, gli edifici storici e monumentali. Con l'utilizzo sempre crescente di nuove tecnologie, è necessario fornire garanzie non solo sulla qualità dei servizi erogati, ma anche sul trattamento delle informazioni che riguardano l'erogazione dei servizi, il personale interno, i Partner, i Clienti e i Fornitori. Infatti le informazioni costituiscono beni aziendali che, in modo analogo agli altri beni, hanno un valore per l'organizzazione e di conseguenza devono essere protetti in modo adeguato. La sicurezza delle informazioni ha il compito di proteggere le informazioni da un ampio numero di minacce in modo da assicurare la continuità del business aziendale, minimizzare i danni e massimizzare il ritorno degli investimenti e delle opportunità commerciali.
Preservare la fiducia che i Clienti hanno nei confronti di A.I.C.E. Consulting S.r.l., richiede che ciascuno contribuisca al rispetto, alla tutela e alla sicurezza di tutti i dati e delle informazioni riservate.
Da questo punto di vista A.I.C.E. Consulting S.r.l. è consapevole e si impegna nel supportare i clienti che ricadono nel perimetro della NIS 2, in relazione agli obblighi derivanti dalla direttiva.
Sebbene A.I.C.E. Consulting S.r.l. non sia direttamente soggetta alla NIS 2, parte suoi clienti lo sono. La NIS 2 pone l'accento sulla sicurezza della catena di fornitura, rendendo essenziale che i fornitori siano allineati con i requisiti di sicurezza dei loro clienti per garantire la continuità operativa e ridurre i rischi.
In questo senso A.I.C.E., all'interno della catena di fornitura, si allinea con i requisiti di sicurezza dei propri clienti per garantire la continuità operativa e ridurre i rischi.

2. Principi

Secondo la definizione dello standard ISO 27001, la sicurezza delle informazioni è caratterizzata dalla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite.
Proteggere la sicurezza di un sistema significa:

- Ridurre ad un valore accettabile la probabilità che vengano violati i parametri di sicurezza informatica;
- Individuare tempestivamente quando ed in quale parte del sistema questo accade;
- Limitare i danni e ripristinare i requisiti violati nel minor tempo possibile.

Supportato da direttive di leadership, il programma di sicurezza di A.I.C.E. Consulting S.r.l. include personale dedicato responsabile dell'implementazione dei controlli di sicurezza in tutte le aree aziendali. Il programma di sicurezza è applicato, monitorato, mantenuto, migliorato e documentato in coerenza con le finalità del business facendo riferimento allo standard internazionale ISO/IEC 27001. L'applicazione del programma di sicurezza richiede l'implementazione, conforme con i requisiti di business aziendali, delle misure di sicurezza che consentono di ridurre i livelli di rischio e l'applicazione delle politiche, processi, procedure, controlli, ecc. che assicurano il rispetto dei requisiti attesi di riservatezza, integrità e disponibilità delle informazioni, oltre che l'ottemperanza delle normative vigenti in materia di sicurezza delle informazioni come ad esempio il backup, il controllo degli accessi e il monitoraggio dei log.

3. Obiettivi

Al fine di poter rispondere in modo efficace ed efficiente alle richieste ed esigenze dei clienti e di garantire la qualità e sicurezza dei servizi erogati, A.I.C.E. Consulting S.r.l. ha adottato le migliori pratiche di settore ed ha realizzato un Sistema di Gestione della Sicurezza delle Informazioni in conformità allo standard ISO 27001.

Il Sistema di Gestione per la Sicurezza Informazioni (ISMS), progettato da A.I.C.E. Consulting S.r.l., si basa su:

- Gestione dei rischi per la sicurezza delle informazioni in sinergia con la gestione del rischio complessivo aziendale e nel rispetto del responsabile utilizzo delle risorse aziendali, realizzata attraverso l'applicazione di modelli condivisi, ripetibili e validi nel tempo, riferibili ai riconosciuti standard internazionali;
- Individuazione dei ruoli organizzativi e delle responsabilità specificamente coinvolti nella gestione della sicurezza delle informazioni;
- Sensibilizzazione del personale alla sicurezza delle informazioni, valorizzazione e formazione delle competenze di maggiore interesse per la sicurezza delle informazioni;
- Monitoraggio continuo dell'efficacia ed efficienza del ISMS attraverso la definizione di un sistema di indicatori e la loro misurazione periodica;
- Impegno della Direzione per fornire le risorse ritenute necessarie per l'attuazione delle politiche aziendali per la sicurezza, il perseguimento degli obiettivi di sicurezza, il mantenimento e miglioramento continuo del ISMS.

Infine dato che è fondamentale sviluppare e gestire una rete sicura, le apparecchiature A.I.C.E. Consulting S.r.l. sono acquistate pensando alla sicurezza e sono soggette a manutenzione periodica. Per garantire la riservatezza delle informazioni, A.I.C.E. Consulting S.r.l. gestisce le comunicazioni sia interne che esterne tramite algoritmi di cifratura e certificati adeguati. Strumenti e metodi aggiornati in termini di sicurezza IT e OT vengono applicati costantemente per ridurre i rischi e affrontare le vulnerabilità in proporzione alle necessità dell'azienda e in ottemperanza alle normative vigenti in materia. Perciò A.I.C.E. Consulting S.r.l. ha adottato un sistema di sicurezza aziendale allineato a best-practice e standard internazionali, volto ad adottare in particolare lo standard ISO-27001 che prevede l'implementazione e l'applicazione di rigide misure di controllo dell'accesso alle informazioni in base al principio "need-to-know" correlato al business aziendale, il monitoraggio e i test regolari del ISMS.

4. Riferimenti agli aspetti normativi

Tutti i requisiti cogenti e contrattuali pertinenti sono identificati dall'organizzazione ed è stato strutturato un processo per assicurare che:

- Gli aggiornamenti normativi relativi alla privacy (GDPR - Regolamento UE 2016/679), siano disponibili e noti alle varie direzioni e funzioni aziendali interessate;
- Gli aggiornamenti relativi alla Direttiva NIS2 e relativa attuazione, siano disponibili e noti alle varie direzioni e funzioni aziendali interessate;
- Vengano effettuati i dovuti aggiornamenti alle procedure operative e ai sistemi informatici aziendali al fine di rispettare le normative vigenti (Compliance).

Il Responsabile dei sistemi informatici assicura il monitoraggio e l'approvazione dell'avvenuta applicazione in azienda degli aggiornamenti normativi.

5. Diffusione della cultura e delle politiche di sicurezza

La sicurezza è un processo che riguarda tutti, la consapevolezza individuale unita ad un utilizzo responsabile delle risorse svolge un ruolo fondamentale nel conseguimento degli obiettivi di sicurezza prefissati. L'impegno di A.I.C.E. Consulting S.r.l. per la sicurezza inizia e termina con i propri dipendenti e con gli stakeholder, pertanto il personale viene sensibilizzato riguardo a tale importanza. La società si impegna a diffondere in azienda una cultura della sicurezza delle informazioni, considerata necessaria per la tipologia di servizi offerti dall'azienda e dei dati trattati. Questo sforzo inizia ai vertici prevedendo la definizione di ruoli e responsabilità e mantenendo viva la consapevolezza, la cultura e la sicurezza aziendale a tutto il personale tramite la diffusione di politiche complete e semplici da comprendere sulla sicurezza dei dati regolarmente comunicate in tutta l'organizzazione attraverso canali di comunicazione interna e tramite sessioni di formazione specifiche o comunicazioni che illustrino l'importanza della sicurezza della catena di fornitura nel contesto della NIS 2 e le implicazioni per i processi aziendali.
La gestione della sicurezza delle informazioni interessa l'intera azienda ed è un'attività significativamente complessa. Sono presenti team dedicati impegnati nella sicurezza IT che assicurano il coordinamento complessivo dell'intero processo di gestione e collaborano per promuovere le migliori pratiche di sicurezza dei dati. È importante che tutti i dipendenti e le terze parti coinvolte nei processi aziendali collaborino per quanto di propria competenza rispettando le regole e le procedure operative riportate nella documentazione del Sistema di Gestione della Sicurezza delle Informazioni (disponibili nella intranet aziendale) e applicando le migliori pratiche ed i migliori comportamenti. Per questo motivo la comunicazione delle politiche di sicurezza aziendali viene estesa ai propri partner, fornitori e clienti all'atto della stipula o rinnovo periodico del contratto. La collaborazione e la comunicazione con partner e fornitori per assicurare la comprensione e l'applicazione delle politiche di sicurezza anche da parte loro diviene fondamentale anche al fine di supportare i requisiti NIS 2 dei clienti.

6. Impegno della leadership

La Direzione favorisce lo sviluppo della cultura aziendale verso l'applicazione delle regole e dei requisiti della sicurezza delle informazioni (a garanzia dell'azienda, dei clienti, dei terzi) e la sensibilizzazione e coinvolgimento di tutte le funzioni aziendali nel contribuire al perseguimento degli obiettivi della sicurezza. La Direzione si impegna, quindi, a fornire le risorse ritenute necessarie per l'attuazione delle politiche aziendali per la sicurezza, il perseguimento degli obiettivi di sicurezza e il mantenimento e miglioramento continuo del Sistema di Gestione della Sicurezza Informazioni prevedendo il riesame delle politiche di sicurezza almeno una volta l'anno o nel caso di variazioni significative di Business o dell'infrastruttura.
La Direzione si impegna a diffondere e mantenere viva la consapevolezza, la cultura e le politiche di sicurezza aziendale a tutto il personale interno ed esterno attraverso diversi canali di comunicazione interna (newsletter, giornate di formazione, distribuzione del Regolamento Informatico che determina le regole ed i comportamenti che vanno seguiti in A.I.C.E. Consulting S.r.l., diffusione della politica per adempiere a leggi e regolamenti, ecc.).

7. Metodologia analisi e gestione dei rischi

La sicurezza deve essere continuamente monitorata perciò A.I.C.E. Consulting S.r.l. ha adottato una metodologia di analisi e gestione del rischio della sicurezza delle informazioni nonché un processo periodico, effettuato annualmente o ogni qualvolta si modifica o implementa un

processo, di gestione dei rischi al fine di mantenere i rischi a un livello accettabile tramite la valutazione e il trattamento degli stessi. Per fare ciò sono stati definiti i criteri per la valutazione e l'accettazione del rischio e identificate in modo oggettivo e trasparente le potenziali minacce e vulnerabilità che possono derivare dalla progettazione, dall'implementazione o dalla gestione dei sistemi e che potrebbero essere sfruttate per compromettere la sicurezza delle informazioni, i relativi danni, sia diretti che indiretti e le misure di protezione in atto, in modo da evidenziare le aree con maggiore criticità e prevedendo l'implementazione di contromisure adeguate.