DOCUMENTO DI POLITICA DELLA SICUREZZA E OBIETTIVI - ANNO 2020

SOMMARIO DEL DOCUMENTO

Il Direttore Operativo e
RdS
Claudio De Persio

STRATEGIA GENERALE

L'azienda ha deciso di predisporre un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) basato sulla norma ISO 27001:2017, da sottoporre a certificazione.
La certificazione è stata ottenuta nel mese di ottobre 2019.
Il SGSI è fondato sui principi fondamentali delineati nella procedura "COBAT_S000 – Descrizione Generale del Sistema di Gestione per la Sicurezza delle Informazioni" (rev. 1 del 01/07/2019).

POLITICA PER LA SICUREZZA

La sicurezza informatica è un processo di impostazione e di gestione delle misure atte a garantire la riservatezza, l'integrità e la disponibilità dei dati in modo conforme alla normativa cogente e alle normative volontarie a cui l'azienda si vuole riferire.
La Direzione attribuisce un'importanza strategica al trattamento delle informazioni e vuole difendere la riservatezza, integrità e disponibilità dell'informazione stessa, sia quando è patrimonio dell'azienda sia quando è patrimonio informativo dei propri clienti.
Nello specifico le linee seguite per la gestione sicura delle informazioni sono:

- proteggere le informazioni da accessi non autorizzati;
- tutelare la riservatezza delle informazioni;
- impedire la concessione di autorizzazioni al trattamento e alla modifica delle informazioni da parte di soggetti non autorizzati;
- garantire la disponibilità delle informazioni agli utenti autorizzati;
- redigere piani dell'attività aziendale costantemente aggiornati e controllati;
- formare il personale in materia di sicurezza delle informazioni;
- analizzare i punti deboli e le violazioni alla normativa vigente.

L'intero processo di gestione delle informazioni prevede il coinvolgimento e l'integrazione di tutti gli elementi che nell'impresa intervengono e creano valore per raggiungere l'obiettivo, ovvero persone, processi e tecnologie al fine di gestire la sicurezza delle informazioni al meglio.

La Direzione intende coinvolgere nel processo di gestione anche due attori esterni importanti per il completamento del quadro complessivo e che sono i Clienti ed i Fornitori.

La sinergia tra essi e l'azienda, anche se con ruoli distinti, è individuata dalla Direzione come un punto di forza del Sistema di Gestione stesso.

La politica viene diffusa sia all'interno che all'esterno intendo essere elemento di impegno per l'azienda al raggiungimento di conformità a specifiche normative ed esigenze dei clienti.

DESCRIZIONE DELL'ORGANIZZAZIONE

Le attività precipue di business aziendali sono le seguenti "Servizi di pianificazione e coordinamento delle attività di raccolta, trasporto e invio a riciclo di rifiuti"
Ai fini della certificazione ISO 27001, pertanto, è stato considerato il seguente scopo:

Gestione dei Sistemi Informativi finalizzati all'erogazione di Servizi di pianificazione e coordinamento delle attività di raccolta, trasporto e invio a riciclo di rifiuti

L'Azienda si propone di gestire le attività incluse nel campo d'applicazione del SGSI, suddividendole per processi, come specificato nel documento "COBAT_S000 – Descrizione Generale del Sistema di Gestione per la Sicurezza delle Informazioni" al paragrafo 6.1.1 e nei correlati Allegati Operativi (facenti parte del SGSI).
Il SGSI si intende applicato per le attività e gli asset collocati all'interno della sede operativa dell'azienda, sia se svolte da personale interno che da personale esterno.
Il SGSI non si applica alle attività svolte all'esterno dell'azienda, presso la sede dei clienti, anche se si dovesse svolgere con il supporto di componenti elettroniche di proprietà dell'azienda, considerato che tali attività sono svolte in promiscuità con personale del cliente e in ambienti su cui non si possono imporre regole di sicurezza dell'azienda.
I beni dell'azienda oggetto del SGSI sono stati censiti come specificato nella procedura "COBAT_S003 – Misure di Sicurezza per i Sistemi Informatici" al § paragrafo 2.1.
L'azienda è dotata di una rete informatica e si avvale, per i servizi di connettività internet e posta elettronica, di fornitori esterni.
L'azienda ha elaborato una propria metodologia dei rischi come indicato nella procedura "COBAT_S005 – Metodologia di valutazione del rischio per la sicurezza delle informazioni"

RISORSE DEDICATE AL SGSI

Il budget economico stanziato dall'azienda per l'anno 2020 allo scopo è il seguente:

- ***** euro (*riservato*), per attività e prodotti strettamente inerenti il SGSI;
- ***** euro (*riservato*), per attività e prodotti riconducibili al SGSI;

Nella prima voce rientrano:

- attività specifica di consulenza per la manutenzione del SGSI;
- lavoro di personale interno, soprattutto Responsabile per la Sicurezza (RdS) e responsabile dei Sistemi Informativi (RSI) volto a supportare la gestione del SGSI;
- accorgimenti di sicurezza fisica per il CED.

Nella seconda voce rientrano:

- server e apparati di rete;
- attività specifica per la configurazione delle componenti di cui al punto precedente;
- lavoro di personale interno, soprattutto responsabile dei Sistemi Informativi (RSI) e tecnici volto a collaudare e manutenere i sistemi.

OBIETTIVI STRATEGICI DELL'ANNO 2020

Sono stabiliti i seguenti obiettivi strategici per il periodo 2020:

- Mantenimento della certificazione ISO 27001:2017
- Avanzamento del processo di integrazione tra i sistemi ISO 9001 e ISO 27001.
- Formazione a tutto il personale in materia di sicurezza delle informazioni.
- Risoluzione delle vulnerabilità emerse in fase di VAPT
- Estensione dei VAPT anche agli applicativi amministrativi
- Svolgimento di tutte le attività necessarie al mantenimento dei rischi di livello Trascurabile o Basso
- Svolgimento di tutte le attività di trattamento del rischio per la diminuzione dei livelli di rischio attualmente Medio o Alto.