I sistemi utilizzati per l'erogazione del servizio sono ospitati presso il data center regionale gestito da Insiel in qualità di Responsabile Esterno al trattamento dei dati personali.

Insiel garantisce il rispetto delle misure minime di sicurezza e ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni, certificato secondo la norma UNI EN ISO/IEC 27001:2014.

Il dettaglio che segue presenta un riassunto degli ambiti di intervento attuati da Insiel per quanto riguarda le misure di sicurezza.

Redazione e adozione di politiche di sicurezza aziendali.

Insiel prevede la presenza di norme aziendali relative alla sicurezza dei sistemi, dei dati, degli accessi e dei comportamenti. La complessità organizzativa aziendale obbliga ad una collaborazione trasversale di gruppi di lavoro che, ognuno per le proprie competenze, norma l'aspetto della sicurezza nei trattamenti e nella gestione dei dati.

Il personale Insiel è tenuto al pieno rispetto delle politiche e degli indirizzi aziendali, al rispetto dei regolamenti tecnici interni, agli obblighi cogenti ed agisce in stretta aderenza ai contratti che regolano i rapporti fra Insiel e Amministrazione Regionale.

Organizzazione della sicurezza delle informazioni.

Insiel Spa ha istituito il servizio IT Security con compiti di consulenza, attività di formazione e sensibilizzazione, partecipazione a gruppi di lavoro aziendali e sovra-aziendali, produzione di linee guida. Il servizio IT Security contempla tecnici certificati ISO 27001 (Sistemi di gestione della sicurezza delle informazion) e CISSP (Certified Information Systems Security Professional).

Gestione dei beni.

Insiel garantisce un puntuale inventario dei beni gestiti: hardware, software e banche dati. La catalogazione dei beni permette di attuare un alto livello di controllo sugli strumenti utilizzati per l'accesso ai dati.

Sicurezza delle risorse umane.

La gestione del personale in Insiel è subordinata alla legislazione vigente, nel rispetto delle normative contrattuali e degli accordi aziendali.

Ai dipendenti viene resa pubblica periodicamente, sui siti web dell'Intranet aziendale le comunicazioni e la documentazione riguardante i temi della sicurezza. Viene inoltre gestita la documentazione tecnica specifica organizzata per aree aziendali. Vengono estese anche ai collaboratori esterni le medesime politiche aziendali sulla sicurezza.

Sicurezza fisica e ambientale.

Insiel opera in più sedi collocate in ambito regionale. Tutte soddisfano i requisiti di cui al D.Lgs.81/2008 *tutela della salute e della sicurezza nei luoghi di lavoro*.

L’accesso fisico alle singole è controllato. I dipendenti utilizzano badge magnetici per gli ingressi e gli ospiti devono venir identificati. Le aree esterne sono sorvegliate da un sistema televisivo a circuito chiuso mediante telecamere dislocate lungo il perimetro; le uscite di sicurezza sono controllate da sensori a contatto che rilevano intrusioni o anomalie.

La sede che ospita il data-center implementa ulteriori misure di sicurezza. È presente un controllo regolare di ronda notturna da parte di un servizio di Guardie Giurate; l'accesso ai locali tecnici è permesso solamente al personale autorizzato. L’intera area è protetta da un impianto automatico di controllo fumi e spegnimento automatico a gas.

Gestione delle comunicazioni e dell'operatività.

Il presente ambito è strettamente correlato alle attività di produzione, pertanto gli interventi effettuati da Insiel sono mirati a contenere quanto più possibile le probabilità di danneggiamento e di accessi impropri alle banche dati gestite. Le strategie messe in atto sono specifiche per ogni dominio considerato.

Per quanto riguarda le risorse hardware, server e postazioni client, sono tutte dotate, compatibilmente con il sistema operativo, di protezione antivirus e accesso mediante autenticazione.

Le banche dati sono ospitate presso il data-center; si avvalgono della protezione ambientale (accessi fisici controllati, sistemi antifumo, ecc.). L'accesso logico è sempre sottoposto ad autenticazione. Le politiche di salvataggio dei dati garantiscono il ripristino nei tempi concordati con il cliente e con gli obblighi previsti dal Codice della privacy.

I supporti non più utilizzati (memorie di massa) vengono periodicamente resi inutilizzabili o distrutti in modo da non essere intelligibili e tecnicamente non ricostruibili.

Il software utilizzato da Insiel viene periodicamente aggiornato in modo da prevenire le vulnerabilità degli strumenti elettronici e a correggerne eventuali difetti.

Le reti Intranet gestite da Insiel dispongono di accessi ad Internet attraverso i quali gli utenti possono accedere a varie risorse (navigazione, ftp, email) secondo criteri e regole stabilite. Le protezioni messe in atto comprendono dispositivi di firewall, di intrusion detection e intrusion prevention. Sono presenti vari livelli di segregazione dei segmenti di rete che garantiscono livelli distinti di interdizione legati alla tipologia dei servizi.

E' attiva la modalità di accesso VPN (Virtual Private Network) quando la comunicazione avviene via internet. Nel caso di VPN di tipo Client to LAN, generalmente si fa riferimento a sistemi di autenticazione Active Directory.

Per quanto riguarda la protezione dei sistemi dall' azione di programmi malevoli Insiel si avvale di più soluzioni per una protezione a livelli. I sistemi salvaguardati comprendono i dispositivi client, i server, la navigazione web, i servizi di posta.

Controllo degli accessi.

Gli accessi logici ai sistemi e alle applicazioni sono sottoposti alle politiche aziendali di assegnazione e revoca delle credenziali di autenticazione e dei profili autorizzativi. E' regolamentato tutto il ciclo di vita della credenziale in relazione all'ambito di intervento di ogni singolo operatore incaricato. Ogni operatore viene informato sul corretto uso delle parole

chiave. Nella gestione delle credenziali di autenticazione sono soddisfatti gli obblighi previsti dal disciplinare tecnico in materia di misure minime di sicurezza del Codice della privacy.

Per quanto riguarda gli amministratori di sistema, Insiel ha adottato quanto previsto dal Provvedimento 27 novembre 2008 del Garante della privacy *Attribuzione delle funzioni di amministratore di sistema*.

Acquisizione, sviluppo e manutenzione dei sistemi informativi.

Le applicazioni utilizzate da Insiel garantiscono un adeguato livello di sicurezza, essendo implementate per verificare l'immissione dei dati, la loro congruità e consistenza, ed impediscono il danneggiamento casuale o volontario delle informazioni trattate. Per quanto riguarda software di terze parti utilizzato nelle procedure di trattamento dei dati Insiel verifica che i prodotti siano conformi a quanto previsto dal Codice della privacy.

Gestione degli incidenti relativi alla sicurezza dei sistemi informativi.

Insiel ha istituito una struttura interna che svolge una attività di gestione, analisi e storicizzazione degli eventi rilevanti per la sicurezza. Il processo prevede la rilevazione degli eventi rilevanti per la sicurezza, la gestione di tali eventi, la risoluzione degli incidenti, la raccolta delle evidenze.

Pianificazione della continuità operativa.

Insiel ha posto in atto una serie di misure operative per garantire la continuità operativa del data-center in caso di incidenti gravi alle risorse hardware e alle strutture fisiche, e nel caso di eventi calamitosi.

Conformità.

Insiel preso atto della legislazione vigente ha provveduto ad applicare le normative sensibilizzando il personale al rispetto degli obblighi.

Interventi Formativi.

L' azienda, in corrispondenza al tipo di attività e ai requisiti cogenti, ha istituito nel corso degli anni percorsi formativi sui temi della sicurezza, sia in senso ampio che specifico, e del rispetto delle normative sulla privacy. La pianificazione della formazione prevede continui aggiornamenti anche a fronte di cambiamento di tecnologie o interventi legislativi.