L'erogazione di servizi in sicurezza e la salvaguardia del patrimonio informativo, nonché l'erogazione di servizi in cloud in modalità sicura e nel rispetto della normativa della privacy, costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di Join.it. I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi dell'organizzazione e il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) rappresenta lo strumento che consente l'individuazione di corrette best practice per il miglioramento costante della condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni a livelli accettabili. In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di disponibilità, integrità e riservatezza delle informazioni attraverso l'adozione di un formale "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI) in linea con i requisiti attesi dagli stakeholder di Join.it.

In particolare, il Sistema di Gestione della Sicurezza delle Informazioni è applicato alla:

"Progettazione ed erogazione di servizi sistemistici on premise e da remoto e sviluppo software in ambito di trasformazione digitale dei processi di business anche erogato in modalità SaaS"
In inglese:
"Design and delivery of on premise and remote system services and software development in digital transformation of business processes also delivered in SaaS mode."

Gli obiettivi generali del SGSI perseguiti con l'impegno della direzione, sono:
- dimostrare ai clienti la propria capacità di fornire con regolarità prodotti/servizi sicuri, massimizzando gli obiettivi di business;
- minimizzare il rischio di perdita e/o indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua ed adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il SGSI;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- promuovere la collaborazione, comprensione e consapevolezza del SGSI da parte dei fornitori strategici;
- conformarsi ai principi e ai controlli stabiliti dalla ISO 27001, ISO 27017 e ISO 27018 o altre norme/regolamenti che disciplinano le attività di business in cui opera l'azienda, tra i quali, in particolare, le regolamentazioni inerenti alla Privacy e la sicurezza dei dati personali (GDPR).

In particolare, per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO 27017, la direzione si impegna ad adottare requisiti di sicurezza che prendano in considerazione i rischi derivanti dal personale interno, la gestione sicura del multi-tenancy (condivisione dell'infrastruttura), l'accesso agli asset in cloud dei clienti da parte del personale del service provider, il controllo degli accessi (in particolare degli amministratori), le comunicazioni ai clienti in occasione di cambiamenti dell'infrastruttura, la sicurezza dei sistemi di virtualizzazione, la protezione e l'accesso dei dati dei clienti in ambiente cloud, la gestione del ciclo di vita degli account cloud dei clienti, la comunicazione degli incidente e dei data breach e linee guida per la condivisione delle informazioni a supporto delle attività di investigazione e forensi nonché la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud.

Inoltre, l'azienda è costantemente impegnata nella protezione dei dati personali degli interessati che gestisce, con particolare riferimento a quelli dei propri clienti. Rispetto a questi ultimi l'azienda, ai sensi della ISO 27018 e in accordo con la legislazione privacy vigente (GDPR), agisce come "*Data Processor*" ovvero come "*Responsabile del Trattamento*" ex art. 28 del GDPR, dichiarando questo status e i relativi

obblighi che ne discendono nei contratti con i clienti. Tali obblighi sono riportati anche nelle nomine a responsabile dei fornitori utilizzati per svolgere il trattamento.
Tutta l'azienda ed i suoi partner sono coinvolti nella segnalazione di eventuali incidenti riscontrati e di qualsiasi debolezza identificata nel SGSI e si impegnano nel supportare l'implementazione, la messa in opera, il riesame periodico ed il miglioramento continuo del SGSI.

La Direzione si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica, con il fine ultimo del miglioramento continuo della sicurezza dei suoi servizi.

AZZARELLO MARIO AGOSTINO
2025.04.29 09:47:59
CN=AZZARELLO MARIO AGOSTINO
C=IT
2.5.4.4=AZZARELLO
2.5.4.42=MARIO AGOSTINO
RSA/2048 bits