Politica di Banca Monte dei Paschi di Siena S.p.A. per il governo della sicurezza logica

Al fine di proteggere il patrimonio informativo aziendale, Banca Monte dei Paschi di Siena S.P.A. ha definito "Sistema di Gestione della Sicurezza delle Informazioni" (di seguito SGSI), adottato a livello di Gruppo, che fornisce un indirizzo generale e strategico di medio/lungo termine in conformità ai principali standard internazionali di riferimento ISO/IEC 2700x (series).

In tale contesto sono indicate le linee guida del processo complessivo di Governo della Sicurezza Logica in termini di:

- definizione strategie e politiche, seguimento e monitoraggio delle misure di sicurezza logica da adottare per proteggere il patrimonio informativo aziendale coerentemente con gli obiettivi di rischio ed i limiti operativi stabiliti nel RAF, anche con la definizione di framework di misurazione e valutazione del raggiungimento degli obiettivi;
- gestione degli incidenti operativi e di sicurezza;
- monitoraggio dell'efficacia delle misure adottate in materia di sicurezza delle informazioni, al fine di implementare un processo di miglioramento continuo;
- definizione e seguimento del piano di formazione e sensibilizzazione sulla sicurezza delle informazioni;
- definizione e monitoraggio delle misure di sicurezza e dei presidi di controllo da adottare per i servizi informatici esternalizzati o forniti da terze parti;
- implementazione delle misure di sicurezza definite e gestione delle piattaforme di sicurezza nel continuo;
- verifica della conformità e del rispetto delle disposizioni di legge in materia di sicurezza informatica, ottemperando alle normative cogenti in materia di data protection quali GDPR e circolare 285 di Banca d'Italia.

I principi di cui sopra sono applicati anche rispetto alle terze parti (fornitori, consulenti, ecc.) che operano nel contesto del Gruppo Montepaschi per quanto di competenza con l'attività svolta.

Il governo della sicurezza logica si interseca strettamente con molti elementi e processi del sistema aziendale (tra i quali Gestione del Rischio ICT e di Sicurezza, Sistema di Gestione della Continuità Operativa, IT Service Continuity, Gestione degli Incidenti).
Si riportano di seguito i principali ambiti di applicazione, in linea con i domini ISO 27001:

- **Politiche di sicurezza informatica**: sono definiti gli indirizzi generali, le linee guida da seguire e gli obiettivi da perseguire che fanno da riferimento per tutte le normative in ambito sicurezza informatica.
- **Organizzazione della sicurezza informatica**: sono definiti ruoli e responsabilità relativi alla sicurezza delle informazioni, in modo da separare compiti e aree di responsabilità in potenziale sovrapposizione; sono definiti relativi framework di sicurezza ed indicatori per l'indirizzo, il controllo e il monitoraggio delle misure di protezione e di salvaguardia dei principi generali del Gruppo MPS; Sono inoltre mantenuti contatti con le autorità competenti e con associazioni di settore per garantire costante allineamento ed info-sharing.
- **Gestione delle risorse umane**: Ogni dipendente del Gruppo Montepaschi e tutte le terze parti coinvolte nei processi produttivi del Gruppo devono adottare un atteggiamento di vigilanza continua in tema di sicurezza delle informazioni e devono adottare, in ogni fase di lavoro, le opportune misure per la sicurezza delle informazioni definite nelle politiche di sicurezza logica del Gruppo; il personale, compreso quello che riveste ruoli chiave, riceve una formazione adeguata sui rischi ICT e di sicurezza, compresa la sicurezza dell'informazione.
- **Gestione degli asset aziendali**: Ogni asset aziendale deve essere valutato almeno in base ai parametri della cd CIA (confidentiality, integrity e availability) cioè confidenzialità, integrità, disponibilità, a cui si aggiunge l'accountability; Tutte le risorse IT, intese come hardware, software, procedure e dati/informazioni appartenenti al Gruppo MPS sono asset aziendali e come tali devono essere protetti.
- **Controllo degli accessi**: la gestione degli accessi ai sistemi e alle applicazioni ICT del Gruppo Montepaschi è delimitata sulla base delle attività operative svolte dagli utenti, coerentemente con il ruolo da loro svolto e nel rispetto delle misure di sicurezza definite; Le procedure per il controllo degli accessi sono applicate, monitorate, periodicamente aggiornate e prevedono controlli per il monitoraggio di eventuali anomalie e opportune contromisure per impedire accessi non autorizzati ai dati.
- **Data security**: sono adottati sistemi e processi che assicurano la confidenzialità disponibilità e integrità delle informazioni quali a titolo di esempio la crittografia;
- **Sicurezza fisica e ambientale**: L'accesso fisico alle strutture centrali dell'Azienda da parte dei dipendenti e dei visitatori (fornitori, collaboratori o clienti) viene autorizzato, tracciato e monitorato al fine di prevenire eventuali accessi indesiderati.

- **Sicurezza operativa**: sono adottati strutture/processi/strumenti volti alla protezione dei dati aziendali in termini di disponibilità, integrità e confidenzialità.
- **Sicurezza delle comunicazioni**: vengono utilizzate soluzioni tecniche di sicurezza che permettono:
  la protezione del traffico sulle reti interne, esterne ed i servizi erogati;
  la sicurezza dell'accesso da parte dei clienti ai servizi erogati tramite canali di self banking e delle operazioni disposte tramite questi canali.
- **Acquisizione, sviluppo e manutenzione del sistema informativo**: viene garantita la realizzazione, l'acquisizione e la manutenzione di sistemi applicativi e infrastrutturali affidabili e sicuri anche richiedendo ai fornitori coinvolti nelle attività di sviluppo e manutenzione software/hardware di seguire processi definiti ed in linea con le politiche di sicurezza del Gruppo MPS.
- **Sicurezza delle terze parti**: Mps adotta un framework di governo delle terze parti finalizzato alla valutazione della sicurezza dei servizi/processi/soluzioni esternalizzati presso provider esterni.
- **Gestione degli incidenti di sicurezza informatica**: sono state definite specifiche responsabilità e processi che garantiscono una rapida, efficace ed ordinata risposta agli incidenti di sicurezza, inclusa la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti, anche in caso di fuoriuscite di informazioni.
- **Gestione della continuità operativa**: è predisposto un modello aziendale di gestione della continuità operativa, che consente la mitigazione degli impatti causati dagli eventi avversi anche catastrofici ed il ripristino della normale operatività, sulla base di livelli definiti.
- **Conformità del SGSI**: Il mantenimento dei livelli di sicurezza è garantito attraverso il monitoraggio dell'efficacia delle misure di sicurezza in essere e con revisioni periodiche del complessivo SGSI.