Politica Sicurezza Informatica e Privacy

Indice Generale

1. Politica della sicurezza

[1] Sagitta SGR S.p.A. (di seguito la “Società” o “Azienda”) ha predisposto questo documento al fine di chiarire l’interpretazione del concetto di sicurezza informatica e privacy e rendere evidenti le proprie politiche in materia.

[2] La tutela degli asset informativi e della privacy dei dati personali, è considerata strategica dall'Azienda; da ciò consegue che soltanto l’utilizzo di strumenti organizzativi e tecnologici in grado di fornire agli asset informativi un adeguato livello di sicurezza e privacy, può consentire all’Azienda di raggiungere i propri obiettivi.

[3] Il concetto di sicurezza informatica e privacy è riferito, in questo contesto, al patrimonio informativo aziendale e concerne la tutela dei seguenti aspetti:

- Integrità;
- Riservatezza;
- Disponibilità.

[4] La tutela di integrità, disponibilità e riservatezza è gestita per mezzo di un **Modello Organizzativo Sicurezza e Privacy** (in seguito, “**MOSP”** o **“Modello”**) integrato con il Sistema di Gestione Aziendale di Sagitta.

[5] Il MOSP ha l’obiettivo di fare in modo che tutte le azioni gestionali ordinarie e straordinarie della società risultino conformi agli standard di mercato e alle norme di legge emanate dallo Stato italiano e dalla Unione Europea (GDPR) in materia di sicurezza applicata al contesto ICT ed ai sistemi informativi e alla privacy dei dati personali.

[6] Il MOSP si ispira allo standard internazionale ISO/IEC 27001-Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni.

[7] I Responsabili del trattamento dei dati (owner del processo) si identificano con i Responsabili di alcuni processi aziendali interni o esternalizzati in base alla mission e responsabilità definite per ciascuno.

La responsabilità dell'impostazione e gestione dei sistemi che garantiscono la sicurezza e la tutela dei dati aziendali e personali, sia dal punto di vista logico sia da quello fisico è demandata alla Direzione aziendale.

Le attività relative alla implementazione, alla gestione ed alla manutenzione del MOSP, di cui questo documento è parte integrante, costituiscono nel loro insieme l'attività di ICT SECURITY E PRIVACY della Società.

La nomina del *Responsabile della Sicurezza Informatica e Privacy* all'interno della Società viene conferita formalmente per mezzo di apposita delibera del CdA.

[8] Questo documento costituisce il principale riferimento per tutti i dipendenti della Società, relativo all'argomento sicurezza informatica e privacy. Essi sono tenuti a farne propri i principi ed i concetti in esso espressi ed a divulgarli, se necessario, a tutte le entità committenti o fornitrici con cui si trovino ad interagire.

Verrà integrato da ulteriori documenti e apposite procedure organizzative per regolamentare le varie attività e i comportamenti del personale.

[9] La presente politica e l'insieme dei controlli adottati a livello aziendale al fine di garantire il perseguimento degli obiettivi di sicurezza informatica e tutela della privacy, sono aggiornati in base alle evidenze derivanti dall'applicazione di metodologie di analisi del rischio. Esse sono applicate alle unità organizzative ed agli asset informativi considerati rilevanti ai fini del perseguimento degli obiettivi e della missione aziendale.

[10] Al fine di perseguire gli obiettivi definiti in questo documento saranno emanati:

- documenti di policy specifiche (Politiche Specifiche di Sicurezza e Privacy) suddivisi per argomento in base alle principali macro aree previste dalla norma ISO/IEC 27001: 2013;

[11] Come analisi del rischio si definisce l'attività che, nel corso della progettazione e della gestione dei prodotti e dei servizi, viene svolta al fine di individuare le minacce relative a ciascun asset informativo e qualificare, successivamente, le contromisure da adottare per contrastarne l'eventuale azione. A livello aziendale viene prevista l'esecuzione di un'analisi dei rischi sicurezza informatica e privacy che consiste

nell'identificazione delle minacce relative a ciascun asset e conduce alla determinazione dell'entità di rischio esistente.

Valori di rischio superiori al rischio target per ciascuna classe di assets, dovranno attivare immediate azioni correttive che verranno pianificate e gestite per mezzo del "Piano Sicurezza Informatica e Privacy".

[12] Al fine di garantire un livello di sicurezza e tutela della privacy adeguato, dovranno essere gestite e mitigate, per mezzo di opportuni controlli, tutte le minacce e tutte le vulnerabilità individuate in quanto la missione della Società non consente di accettare rischi non sottoposti ad azioni di mitigazione o sottoposti esclusivamente ad azioni di trasferimento.

[13] Con apposito ordine di servizio viene resa nota un'apposita "Struttura Organizzativa per la Sicurezza Informatica e Privacy" (Organigramma Privacy) avente l'obiettivo di gestire ed assicurare una comune visione dello stato della sicurezza logica e fisica relativa a tutti gli asset aziendali ivi compresi anche i dati personali, sotto gli aspetti gestionali, progettuali e strategici.

In particolare, all'interno della Struttura Organizzativa, ai fini della gestione delle problematiche di continuità operativa e disaster recovery, viene definito un comitato *ad hoc* chiamato "Comitato di Gestione dell'Emergenze SGR" (si veda documento "Piano di BC & DR Sagitta"), che ha il compito di valutare periodicamente la qualità e completezza dei sistemi di protezione logica e fisica e di individuare le attività di miglioramento, di stabilizzazione e di sviluppo degli stessi. Essa al riguardo produce una relazione destinata al CDA.

Tale comitato si riunisce anche come Gruppo di Crisi al verificarsi di possibili eventi disastrosi o di problemi di impatto rilevante sui servizi erogati e ha l'ulteriore compito di rivedere ed adeguare su base annuale la Politica della Sicurezza e Privacy secondo il divenire delle esigenze della Società.

[14] La selezione dei controlli e, in particolar modo, la definizione delle modalità implementative dei controlli stessi, dovrà essere eseguita tenendo nella debita considerazione la relazione *costo del controllo vs azione mitigatrice ottenuta*.

A questo principio si ispirano anche i controlli e le azioni di monitoraggio implementati per ottemperare alle prescrizioni del GDPR.

[15] Per quanto concerne l'adozione di politiche finalizzate a garantire la continuità dei servizi erogati e dei processi di produzione, gli owner dei processi di business e la

direzione aziendale definiscono, con l'ausilio del Responsabile Securezza Informatica e Privacy esterno, politiche e soluzioni adeguate ai contesti di volta in volta presi in esame, individuate nel rispetto dell'analisi del rischio eseguita a livello aziendale (gestione degli incidenti - business continuity e disaster recovery).

[16] È previsto che tutto il personale sia sottoposto ad un continuo processo di sensibilizzazione e formazione relativo alle problematiche della sicurezza informatica e privacy. Gli interventi formativi saranno definiti nell'ambito di un apposito Piano di Formazione e saranno diversificati in base ai differenti ruoli e competenze assegnate nel contesto aziendale. Il compito di coordinare gli interventi formativi relativi al MOSP spetta alla direzione aziendale con il contributo del Responsabile Sicurezza Informatica e Privacy esterno.

[17] La facoltà di autorizzare deroghe ai principi sanciti nell'ambito del presente documento e, più in generale, alle regole definite nell'ambito del presente MOSP, compete al Responsabile della Sicurezza Informatica e Privacy. In ogni caso le eventuali deroghe concesse, dovranno essere adeguatamente tracciate, motivate e segnalate alla direzione aziendale.

2. Informazioni di configurazione

Area:	Direzione Generale
Ufficio/Funzione:	Sicurezza Informatica e Privacy (esterna)
Attività: Approvato da : Codice Documento: Distribuzione :	Sicurezza Informatica e Privacy Claudio Nardone _____ _____ (Data) (Firma) MOSP_Politica Sicurezza Informatica e Privacy-SAGITTA.doc INTERNA

3. Storia delle modifiche

Versione 1: maggio 2018

Versione 2: gennaio 2021