POLITICA AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI

0	08.11.18	Prima Emissione	RQA		DIR	
n°	**Data**	**Natura Revisione**	**Funzione**	**Firma**	**Funzione**	**Firma**
Dettagli sulla revisione			**Preparato e Verificato**		**Approvato**	

Indice

1. Premessa

Il Sistema Informativo (inclusivo delle risorse tecnologiche - hardware, software, dati, documenti elettronici, reti telematiche - e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi della Società, in considerazione della criticità dei processi aziendali che dipendono da esso.
Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza informatica ed è approvato da DIR e sarà revisionato periodicamente sia in caso di eventi esogeni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi e sulla sicurezza informatica. Le revisioni sono approvate da DIR.

2. Politiche aziendali sui sistemi informativi

Soleto Spa, con sede in via Don Giovanni Minzoni 1 a Milano è uno dei pricipali system integrator presente sul mercato in ambito TLC e ICT. Le informazioni ed i requisiti di sicurezza delle informazioni sono allineati con gli obiettivi aziendali ed il Sistema di Gestione per la Sicurezza delle Informazioni è destinato a essere un meccanismo di abilitazione della condivisione delle informazioni per l'operatività della Società e per ridurre i rischi relativi alle informazioni a livelli accettabili Tutti i dipendenti dell'organizzazione sono tenuti a rispettare le presenti politiche e l'intero Sistema di Gestione per la Sicurezza delle Informazioni. Anche alcune terze parti, individuate da DIR, saranno tenute a rispettarle. La politica sarà riesaminata ogniqualvolta sarà necessario e comunque almeno una volta all'anno in sede di riesame della Direzione. La presente politica riguarda la gestione e l'utilizzo del sistema informativo in tutti i suoi aspetti. Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati requisiti:

- riservatezza: le informazioni devono essere conosciute solo da coloro che ne hanno il relativo diritto, rispettando il principio del minimo privilegio ("necessità di sapere") in base alle mansioni ricoperte ("necessità di operare");
- integrità: le informazioni devono essere precise e complete, devono rispettare i valori e le aspettative aziendali, e devono essere protette da modifiche e cancellazioni non autorizzate. Per soddisfare tale requisito le informazioni devono essere esatte, aggiornate e leggibili;
- disponibilità: le informazioni devono essere disponibili quando richiesto dai processi aziendali, in maniera efficiente ed efficace;
- efficacia: le informazioni devono essere rilevanti e pertinenti al processo aziendale e, allo stesso tempo, devono essere disponibili tempestivamente, senza errori e fornite in modo da poter essere utilizzate dall'utente;
- efficienza: le informazioni devono essere fornite attraverso l'uso ottimale delle risorse sia dal punto di vista della produttività che della economicità;
- affidabilità: le informazioni devono essere appropriate, in modo da permettere ai vertici aziendali di gestire l'azienda e garantire la corretta assunzione delle decisioni; allo stesso modo le informazioni fornite ai responsabili delle varie funzioni devono permettere loro di espletare le loro funzioni, gli obblighi di produzione del bilancio e tutti i report e relazioni previste dalla normativa interna ed esterna.

La gestione del Sistema Informativo aziendale è svolta da personale qualificato che per esperienza, capacità e affidabilità fornisce garanzia del pieno rispetto delle disposizioni interne e delle normative esterne in materia.
I dati personali devono essere trattati:

- in osservanza dei criteri di riservatezza;
- in modo lecito e secondo correttezza;
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- In osservanza alle disposizioni legislative in materia di Privacy

Per poter gestire in modo adeguato il Sistema Informativo è essenziale un efficace processo di monitoraggio che faciliti la pronta individuazione e correzione di eventuali carenze relative a politiche, processi e procedure. Ciò può ridurre considerevolmente la frequenza e/o gravità degli eventi dannosi.

La Società attiva unità organizzative interne che assicurano l'esecuzione di processi atti a:

a) diffondere il contenuto dei servizi, conoscere i punti di forza e di eventuale debolezza;
b) assicurare agli utenti formazione e accesso alle funzioni secondo criteri di sicurezza aderenti a principi di sana e prudente gestione o comunque alle politiche di gestione del rischio informatico;
c) attivare processi volti alla valorizzazione delle risorse informatiche, intese come leva per il raggiungimento degli obiettivi della Società;
d) realizzare un sistema di comunicazione dei fabbisogni o delle criticità del Sistema Informativo con l'obiettivo di attivare un processo di miglioramento continuo;
e) attuare controlli finalizzati a valutare la capacità dell'azienda di attenersi alle politiche interne;
f) individuare tempestivamente deviazioni (anomalie, malfunzionamenti, differenze rispetto a quanto conosciuto/approvato/autorizzato);
g) favorire azioni correttive
h) Attuare tutte le azioni necessarie al miglioramento continuo della sicurezza delle informazioni

La Società predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery. Deve essere sempre assicurata la protezione dei dati e dei sistemi contro le possibili conseguenze dell'attività di software dannoso (c.d. Malware).

Inoltre, la Società, tenuto conto della particolare criticità dei ruoli connessi alla gestione del Sistema Informativo, in particolare del ruolo di "Amministratore di Sistema", adotta delle cautele volte a prevenire e ad accertare eventuali utilizzi non in linea con gli obiettivi aziendali del Sistema Informativo, inefficienze dello stesso, accessi non consentiti ai dati, in specie quelli realizzati con abuso della qualità di Amministratore di Sistema.

La Società, valuta con particolare cura l'attribuzione di funzioni tecniche inerenti la gestione del Sistema Informativo, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche,

professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile, che possono derivare in caso di incauta o inidonea designazione.

L'attribuzione delle funzioni relative alla gestione del Sistema Informativo o alla gestione delle sue componenti si svolge previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni interne ed esterne anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

Nel ricorso ai servizi dei fornitori esterni, la Società utilizza analoghi criteri di valutazione di esperienza, capacità ed affidabilità del fornitore nello svolgimento dell'incarico affidato e della garanzia fornita del pieno rispetto delle vigenti disposizioni di legge, anche quelle in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza.

3. Policy di sicurezza informatica

3.1 Scopo e Ambito di Applicazione

La presente Policy di Sicurezza Informatica costituisce un insieme di riferimenti, in termini di principi di sicurezza e di pratiche da adottare, attraverso il quale la Società intende assicurare la tutela del proprio Sistema Informativo, delle risorse informatiche – informazioni incluse. L'attuazione dei suddetti principi e pratiche di sicurezza tiene conto degli specifici obiettivi strategici e, secondo il principio di proporzionalità, della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati, nonché del livello di automazione dei processi e servizi della Società.

Inoltre, la Società definisce i principi generali di gestione della sicurezza delle informazioni che intende adottare e le principali linee guida di gestione della sicurezza informatica che va dall'analisi dei rischi informatici, alle misure di sicurezza da adottare per proteggere il patrimonio informativo, alla gestione degli incidenti di sicurezza informatica, sino alla definizione delle linee guida per la formazione e comunicazione per il personale e per i clienti in tema di sicurezza delle informazioni. Nella Policy sono anche definite le metodologie necessarie per consentire un controllo dell'efficacia delle misure adottate al fine di implementare un processo di miglioramento continuo.

La presente Policy di Sicurezza Informatica individua i requisiti minimi che si devono osservare nella gestione e nell'utilizzo del Sistema Informativo della Società e applicabili a tutte le unità organizzative della struttura. La stessa deve essere conosciuta, compresa e attuata - per quanto di competenza - da tutto il personale interno e dalle terze parti che sono coinvolte nella gestione di informazioni e componenti del Sistema Informativo.

Nella gestione e nell'utilizzo del Sistema Informativo si deve preservare la sicurezza delle informazioni e dei beni aziendali e si deve assicurare per ciascuna risorsa informatica:

a) una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e responsabilità, appropriata e coerente lungo l'intero ciclo di vita;
b) gli adeguati criteri, modalità di gestione ed utilizzo conformi alle norme di legge e a regolamenti interni ed esterni;
c) la riduzione dei rischi IT mediante misure di prevenzione e di mitigazione, in linea con la propensione al rischio informatico definito a livello aziendale.

Il perseguimento degli obiettivi di sicurezza è conseguito attraverso la definizione, l'attuazione e

l'aggiornamento periodico delle procedure e altri documenti del SGI, dove sono stabilite le misure e le attività volte a:

a) garantire un appropriato livello di confidenzialità/riservatezza delle informazioni;
b) garantire, nel tempo, la disponibilità delle informazioni e dei servizi in linea con gli obiettivi aziendali. A tal fine devono essere implementati adeguati sistemi che assicurino il salvataggio ed il ripristino della disponibilità dei dati (back up);
c) assicurare e mantenere l'integrità delle informazioni;
d) assicurare l'autenticità dei dati, delle transazioni, delle comunicazioni e dei documenti gestiti;
e) garantire l'adeguata formazione e sensibilizzazione del personale sugli aspetti di sicurezza informatica e dell'utilizzo del Sistema Informativo aziendale in modo che tutto il personale della Società contribuisca al raggiungimento di un elevato livello di protezione del patrimonio aziendale e di qualità nell'ambito delle attività quotidiane. La sensibilizzazione del personale alla sicurezza ed alla qualità costituisce condizione necessaria per l'implementazione del Sistema di Gestione per la Sicurezza delle Informazioni e per la definizione, l'attuazione di adeguati controlli di sicurezza nell'ambito della Società. Le relative attività saranno declinate nel piano formativo aziendale.
f) assicurare che le risorse informatiche siano protette contro l'uso non autorizzato;
g) soddisfare e mantenere gli obiettivi e i requisiti definiti dalle normative vigenti;
h) assicurare la gestione ed il monitoraggio degli incidenti relativi al Sistema Informativo, in particolare la gestione degli incidenti di sicurezza informatica.

L'adeguatezza dei processi, delle misure e dei presidi di sicurezza da realizzare ai fini degli obiettivi sopra elencati sono stabiliti sulla base della valutazione dei rischi ICT effettuata periodicamente tramite l'analisi del rischio informatico in relazione con il quadro generale di gestione dei rischi della Società.
Con l'analisi del rischio informatico, la Società individua il livello di efficacia ed intensità dei controlli di sicurezza informatica da adottare e le relative modalità di attuazione. A tale scopo, nell'ambito del documento "Analisi del rischio relativo alla sicurezza delle informazioni" (Risk assessment), la Società prevede l'analisi dei rischi di sicurezza informatica nell'ambito del processo di gestione del rischio informatico.

3.2 Principi generali di sicurezza informatica

Al fine di garantire il raggiungimento degli obiettivi fissati, la Società ha definito i seguenti principi generali di sicurezza da adottare nell'ambito di tutti i processi e delle attività svolte dal personale interno ed esterno. La Società protegge, al massimo livello delle proprie capacità tecniche e delle risorse disponibili, il proprio patrimonio aziendale, articolato nei seguenti elementi fondamentali: persone, beni (asset) e informazioni.

La condizione necessaria per lo svolgimento di ogni attività della Società è la tutela delle informazioni gestite mediante criteri, misure e controlli di sicurezza proporzionali ai rischi e al valore delle informazioni stesse. I controlli di sicurezza da realizzare a tutela delle risorse informatiche che costituiscono il proprio patrimonio sono conseguiti tramite:

a) l'implementazione ed il rispetto delle politiche in tutti gli ambiti organizzativi, procedurali e tecnologici in modo omogeneo rispetto agli obiettivi definiti;
b) l'adeguata attribuzione di compiti e responsabilità all'interno dell'azienda per l'attuazione delle politiche;
c) la verifica (nell'ambito dell'analisi del rischio informatico) del livello di efficacia delle misure realizzate.

d) Il miglioramento continuo del SGSI sulla base dei risultati ottenuti

La Società ha identificato come aree di controllo tutti gli ambiti organizzativi, procedurali e tecnologici rilevanti per l'attuazione dei controlli di sicurezza che consentono il raggiungimento degli obiettivi di sicurezza.
La Policy di Sicurezza Informatica deve essere implementata in accordo con le normative nazionali sia vigenti, sia successive alla data di adozione della presente. In caso di contrasto o omissione, le suddette normative devono essere ritenute prevalenti. La Società attribuisce puntualmente ed in modo non ambiguo i ruoli e le responsabilità in materia di sicurezza al personale (accountability).
L'accountability è condizione necessaria per l'implementazione del Sistema di Gestione per la Sicurezza delle Informazioni e per il raggiungimento ed il mantenimento nell'ambito della Società degli obiettivi di sicurezza definiti. In tale ambito, la Società provvede a verificare che l'operato del personale sia conforme con la presente Policy di Sicurezza.
Al fine di garantire lo svolgimento dell'operatività in situazioni di crisi, la Società ha definito ed implementato il Piano di Continuità Operativa basato su un'appropriata identificazione dei processi critici, delle potenziali minacce che possono realizzarsi su di essi e delle contromisure da adottare. Il Piano di Continuità Operativa è testato e aggiornato regolarmente al fine di garantirne l'efficacia nel tempo.