POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Versione	Data	Autore	Classificazione
2.0	15/01/2024	Davide Persetti	Pubblico
1.0	18/05/2023	Davide Persetti	Pubblico

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 dal CEO 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 dal CEO.

2. OBIETTIVI AZIENDALI SUI SISTEMI INFORMATIVI

Il CEO della Società **KEIS**DATA s.r.l., con sede in Via Carlo Pisacane, 20025 Legnano (MI), che esegue attività di progettazione, sviluppo e manutenzione della piattaforma software **KRC®**, erogazione di servizi di Hosting e SaaS, si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutte le informazioni (in formato elettronico e non) in tutta l'organizzazione al fine di mantenere il proprio vantaggio competitivo, solidità economica, redditività, conformità ai requisiti applicabili (legali, contrattuali ed altri) e immagine commerciale. Le informazioni ed i requisiti di sicurezza delle informazioni continueranno ad essere 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 saranno tenute a rispettarle. La politica sarà riesaminata ogni qualvolta sarà necessario e comunque almeno una volta all'anno.
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 e dai clienti, 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 e 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.

3. MIGLIORAMENTO CONTINUO

La Società si impegna nel miglioramento continuo del proprio sistema di gestione della Sicurezza delle Informazioni.

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 si avvale del servizio cloud fornito da Microsoft tramite la piattaforma Azure, e per il servizio di trasmissione dati dalla società Cloud Italia.

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

- diffondere il contenuto dei servizi, conoscere i punti di forza e di eventuale debolezza;
- 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;
- attivare processi volti alla valorizzazione delle risorse informatiche, intese come leva per il raggiungimento degli obiettivi della Società;
- realizzare un sistema di comunicazione dei fabbisogni o delle criticità del Sistema Informativo con l'obiettivo di attivare un processo di miglioramento

continuo;
- attuare controlli finalizzati a valutare la capacità dell'azienda di attenersi alle politiche interne;
- individuare tempestivamente deviazioni (anomalie, malfunzionamenti, differenze rispetto a quanto conosciuto/approvato/autorizzato);
- favorire azioni correttive.

La Società predispone ed implementa il proprio Piano di Continuità Operativa ed il Piano di Disaster Recovery in modo tale da assicurare 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.

4. POLICY DI SICUREZZA INFORMATICA

4.1 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:

- una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e responsabilità, appropriata e coerente lungo l'intero ciclo di vita;
- gli adeguati criteri, modalità di gestione ed utilizzo conformi alle norme di legge e a regolamenti interni ed esterni;
- 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 Sistema di Gestione, dove sono stabilite le misure e le attività volte a:

- garantire un appropriato livello di confidenzialità/riservatezza delle informazioni;
- 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);
- assicurare e mantenere l'integrità delle informazioni;
- assicurare l'autenticità dei dati, delle transazioni, delle comunicazioni e dei documenti gestiti;
- 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.
- assicurare che le risorse informatiche siano protette contro l'uso non autorizzato;
- soddisfare e mantenere gli obiettivi e i requisiti definiti dalle normative vigenti;
- 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, la Società prevede:
- l'integrazione della gestione dei rischi di sicurezza informatica nell'ambito del processo di gestione del rischio informatico;
- il processo di gestione del rischio informatico e le modalità con le quali è svolta l'analisi del rischio, comprendendo in esso le seguenti attività:
    - censimento e classificazione delle risorse informatiche in termini di rischio informatico;
    - valutazione del rischio potenziale cui sono esposte le risorse informatiche; tale attività interessa altresì tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del Sistema Informativo e si avvale delle informazioni disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato;
    - trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale;
    - accettazione del rischio residuo e/o adozione di misure alternative o ulteriori di trattamento del rischio, qualora il rischio residuo ecceda la propensione al rischio informatico.

4.2 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) ed 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:

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

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 od 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.

Le autorizzazioni di accesso ai dati devono essere strettamente legate alle esigenze informative (necessità di sapere) e alle esigenze operative (necessità di operare) per lo svolgimento dei compiti attinenti al proprio ruolo aziendale. Gli utenti devono essere abilitati soltanto per l'esercizio delle funzioni necessarie allo svolgimento delle loro mansioni. I dati non devono essere condivisi, comunicati o inviati a persone che non hanno la necessità di trattare quei dati per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno della struttura e comunque a soggetti terzi se non previa autorizzazione.

Le attività che comportano rischi significativi per la Società, ove le soluzioni tecniche lo consentono, devono essere organizzate in modo da prevedere il concorso di più soggetti, con responsabilità formalmente ripartite, al fine di evitare l'accentramento delle stesse su una singola risorsa, garantendo un adeguato sistema di controlli incrociati.

La Società implementa apposite misure atte a garantire una pronta, efficace e corretta risposta al concretizzarsi degli incidenti di sicurezza. In tal senso, la Società attua, ove possibile, misure atte a mitigare i potenziali impatti degli incidenti e il ripristino della situazione iniziale in tempi brevi. La gestione degli incidenti prevede opportune procedure di escalation e di reporting in relazione alla gravità degli eventi occorsi.

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.

4.3 Ruoli e Responsabilità in tema di sicurezza informatica

4.3.1 CEO

Assume la generale responsabilità di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali per la sicurezza informatica.

4.3.2 Direzione Generale

È responsabile della gestione della sicurezza informatica, assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica e fornisce informazioni al CEO. In caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti.

4.3.3 Funzioni per la Sicurezza Informatica

Tutti i Responsabili di Area sono deputati allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT.

4.4 Analisi del rischio informatico

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio.
Tale attività interessa:

- tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del Sistema Informativo;
- le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo (ovvero realizzate antecedentemente all'entrata in vigore della presente Policy).

Il processo di analisi è svolto dal Security Manager con il supporto dei Responsabili di Area.
I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza del CEO.

4.5 Controlli di sicurezza nell'ambito dei processi ICT

Con l'obiettivo di garantire un'efficace attuazione della presente policy, la Società definisce ed implementa appositi controlli di sicurezza nell'ambito dei processi operativi dell'ICT.

In particolare, ai fini della presente policy, la Società prevede:

- la gestione dei cambiamenti delle applicazioni e risorse ICT - posta sotto la responsabilità della Direzione Generale - tramite procedure formalmente

definite per garantire il controllo su modifiche, sostituzioni o adeguamenti tecnologici, in particolare nell'ambiente di produzione;

- la valutazione delle iniziative di ampio impatto sul Sistema Informativo (ad es., modifiche rilevanti sulle componenti critiche, adeguamenti in conseguenza di cambio dell'assetto societario, migrazione ad altre piattaforme informatiche) – che si inseriscono di norma in piani strategici approvati dalla Direzione Generale. In tali casi la Società prevede, altresì, la predisposizione di idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela;
- flussi informativi verso i vari livelli manageriali e gli Organi aziendali per il monitoraggio dell'avanzamento delle iniziative di ampio impatto sul Sistema Informativo;
- la gestione degli incidenti di sicurezza informatica con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti.
- la redazione e la tenuta di adeguata documentazione relativa alla gestione degli incidenti informatici intercorsi, da rendere disponibile anche ai fini dell'analisi del rischio informatico;
- l'aggiornamento del Piano di Continuità Operativa per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale ovvero a catastrofi estese che colpiscono la Società o sue controparti rilevanti;
- il raccordo delle procedure di gestione degli incidenti con le attività di monitoraggio di sicurezza di sistemi, accessi e operazioni, nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni;
- la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti nel caso di gravi incidenti di sicurezza informatica e/o nel caso di fuoriuscita di informazioni;
- le comunicazioni al Garante per la protezione dei dati personali in caso di gravi incidenti secondo le modalità previste.

4.6 Comunicazione

La presente Policy di Sicurezza Informatica viene pubblicata sulla intranet aziendale per assicurarne la conoscenza da parte di tutto il personale e viene resa disponibile a tutte le terze parti coinvolte nella gestione di informazioni e componenti del Sistema Informativo.

Nell'eventualità di violazione della presente policy e delle norme attuative, saranno applicate - secondo il caso - le sanzioni previste dal Contratto Collettivo Nazionale applicabile.

CEO **KEIS**DATA s.r.l.
Silvia Cerlesi