N°	DATA	DESCRIZIONE DELLE REVISIONI	PARAGRAFI REVISIONATI
0	**02/10/24**	**PRIMA STESURA**	**Tutti**
1	**15/10/26**	**RIEMISSIONE A SEGUITO AMPLIAMENTO AMBITO SISTEMA PER LA SICUREZZA DELLE INFORMAZIONI**	**Tutti**

POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Obiettivo: garantire la continua idoneità, adeguatezza, efficacia della direzione e supporto per la sicurezza delle informazioni in conformità con i requisiti aziendali, i requisiti legali, statutari, normativi e contrattuali.

La politica generale per la sicurezza delle informazioni e le politiche specifiche devono essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale e dalle parti interessate pertinenti, nonchè riesaminate ad intervalli pianificati e nel caso in cui si siano verificati cambiamenti significativi.

CAE Spa, consapevole che le informazioni trattate costituiscono un patrimonio aziendale ha predisposto ed approvato una politica di prevenzione e protezione.

L'attuazione della politica di prevenzione e protezione si basa sulle risultanze di idonee valutazioni dei rischi, per individuare minacce, vulnerabilità del sistema, probabilità di accadimento di eventi che impattano negativamente sulla sicurezza.

CAE Spa ha approvato la presente politica per la sicurezza delle informazioni.

CAE Spa è consapevole che per lo sviluppo del proprio mercato, il SGSI riveste un ruolo di assoluta rilevanza strategica e rappresenta un importante bene aziendale da tutelare.

In particolare le informazioni rappresentano un patrimonio aziendale e come tale devono essere protetti in modo adeguato.

CAE Spa ha quindi implementato un Sistema di Gestione per la Sicurezza delle informazioni individuando anche i connessi strumenti organizzativi, gestionali e di controllo. L'obiettivo generale è proteggere i dati dalle minacce al fine di:

a) Garantire la continuità gestionale;
b) Minimizzare i danni gestionali;
c) Massimizzare la redditività degli investimenti e le opportunità di mercato;

La sicurezza delle informazioni è intesa come mantenimento di :

a) **riservatezza** ossia garantire l'accesso alle informazioni solo alle persone autorizzate;
b) **integrità** ossia salvaguardare la precisione e la completezza delle informazioni e dei metodi di elaborazione;
c) **disponibilità** ossia garantire l'accesso alle informazioni e ai relativi patrimoni informativi agli utenti autorizzati che lo richiedono;

La riservatezza, l'integrità e la disponibilità delle informazioni sono obiettivi fondamentali per assicurare trasparenza e obiettività, per conseguire e mantenere un margine di competitività, cash-flow, redditività, conformità legale oltre ad una affidabile immagine commerciale.

La sicurezza delle informazioni è ottenuta implementando una serie di controlli idonei quali Manuale di Gestione della Sicurezza delle informazioni, disposizioni organizzative, procedure gestionali ed operative, procedimenti ed istruzioni, strutture organizzative e funzioni software. Questi controlli sono stati stabiliti per garantire il rispetto degli obiettivi specifici che mirano alla protezione del patrimonio CAE Spa.

La sicurezza raggiungibile solo attraverso i mezzi tecnici è limitata e deve essere supportata da una gestione e da procedure adeguate. La sicurezza e i suoi controlli esigono una attenta e sistematica pianificazione, unitamente ad una meticolosa cura del particolare.

La gestione della sicurezza delle informazioni è il risultato tangibile di una partecipazione competente e responsabile anche di fornitori e clienti.

I requisiti di sicurezza sono stati identificati mediante il ricorso a tre fonti principali.

Prima fonte : la valutazione dei rischi. Questa fonte ha consentito di individuare le minacce, valutare la vulnerabilità e la probabilità di accadimento delle minacce oltre a stimarne l'eventuale impatto.

Seconda fonte : i requisiti legali, prescritti da leggi, norme regolamentari e contrattuali che CAE Spa, deve soddisfare.

Terza fonte : una specifica serie di principi, obiettivi e requisiti per il trattamento e l'elaborazione dei dati che CAE Spa ha sviluppato per supportare le proprie attività e a valle della valutazione dei rischi.

Il Responsabile della Sicurezza delle informazioni, esegue revisioni periodiche della valutazione dei rischi di protezione e dei controlli implementati per :

a) prendere in considerazione le modifiche ai requisiti gestionali e alle priorità;
b) prendere in considerazione nuove minacce e vulnerabilità;
c) confermare che i controlli siano validi e idonei ed efficaci.

Vengono eseguite revisioni periodiche ogni qualvolta necessarie, in base ai risultati di valutazioni precedenti e per confronto ai livelli di rischio stabiliti. In particolare, sono implementate revisioni periodiche e/o estemporanee, quando necessario, dei seguenti fattori:

- l'efficacia della politica per la sicurezza delle informazioni dimostrata dalla natura, numero e incidenza degli accadimenti dannosi registrati;
- il costo e l'incidenza dei controlli sull'efficacia gestionale;
- gli effetti delle modifiche apportate alla tecnologia;

CAE Spa ritiene critici per un'implementazione positiva della sicurezza delle informazioni i seguenti fattori:

a) la politica di sicurezza delle informazioni e le attività che riflettono gli obiettivi gestionali in essa contenuti;
b) la conformità ai regolamenti sulla Privacy (GDPR), NIS2, AI ACT e CRA;
c) l'approccio per un'implementazione della sicurezza delle informazioni coerente con la cultura di CAE Spa
d) la buona comprensione dei requisiti di sicurezza, valutazione e gestione dei rischi
e) la distribuzione ai fornitori di direttive per l'attuazione delle norme e della politica di sicurezza delle informazioni;
f) la garanzia di addestramento e formazione inerenti la sicurezza delle informazioni
g) un sistema di misurazione per valutare le prestazioni di gestione della sicurezza delle informazioni e suggerimenti per il miglioramento continuo.

Questi fattori critici di successo per la gestione della sicurezza delle informazioni impegnano CAE Spa dalla gestione di tale sistema ad un approccio organizzativo che include le seguenti direttive :

a) la conformità ai requisiti legislativi e contrattuali
b) la prevenzione e rivelazione di software non autorizzati
c) la gestione della continuità operativa;
d) le conseguenze della violazione della politica di sicurezza;
e) una definizione delle responsabilità gestionali e specifiche per la gestione della sicurezza delle informazioni
f) la verbalizzazione di incidenti inerenti la sicurezza delle informazioni;
g) la documentazione organizzativa, gestionale e operativa a supporto della politica della sicurezza delle informazioni;
h) la divulgazione in forma adeguata, accessibile e comprensibile agli operatori e agli utenti, delle direttive e procedure di sicurezza;
i) la sistematica e periodica valutazione dei rischi come attività preventiva;
j) la eliminazione dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non è possibile, loro riduzione al minimo;
k) la riduzione dei rischi alla fonte;
l) la programmazione della prevenzione che integri in modo coerente le condizioni tecniche, produttive e organizzative nonché l'influenza dei fattori dell'ambiente di lavoro
m) la sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
n) la priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;

CAE Spa si impegna al pieno adeguamento ai requisiti di legislazione in tema di protezione dei dati anche relativamente ai trattamenti di dati dei suoi clienti in qualità di Responsabile del trattamento secondo quanto previsto in modo trasparente nelle clausole contrattuali siglate fra le Parti (che specificano chiaramente la tipologia del servizio cloud offerto – modalità SaaS).

In ambito di fornitura del servizio SaaS, CAE Spa ha come punto di riferimento l'implementazione della seguente politica:

- i servizi in cloud sono progettati e implementati tenendo conto di misure tecniche di sicurezza nella gestione delle informazioni;
- viene fatta un'analisi relativa ai rischi di attività condotte anche da coloro che hanno le autorizzazioni a gestire i servizi in cloud sul cliente;
- separazione e isolamento (inclusa la virtualizzazione) degli spazi per i dati dei diversi Clienti;
- definizione dei controlli degli accessi e permessi da parte degli utenti autorizzati a lavorare sui diversi Cloud services dei Clienti;
- un flusso comunicativo definito con il Cliente di gestione di eventi di change management;
- implementazione di politiche di virtualizzazione sicura;
- formazione continua al personale e procedure mirate a preservare la sicurezza dei dati del Cliente;
- sensibilizzazione a tutti coloro che svolgono attività per la fornitura dei servizi Cloud sul Cliente delle procedure di Data breach e dei processi di investigazione in presenza di violazione del trattamento dei dati.

Il documento di Politica per la sicurezza delle informazioni viene riesaminato ad intervalli prestabiliti. Questo di regola avviene in occasione del riesame annuale da parte della Direzione del SGSI. Il documento viene riesaminato al di fuori di questa periodicità anche in occasione di cambiamenti significativi dell'organizzazione (pianificati o straordinari) al fine di verificarne la sua continua idoneità, adeguatezza ed efficacia.