

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

In conformità alla norma ISO/IEC 27001:2022 e alle Linee Guida
ISO/IEC 27017:2021 E ISO/IEC 27018:2020



STATO DELLE REVISIONI DELLA POLITICA SICUREZZA DELLE INFORMAZIONI:

REV	DESCRIZIONE MOTIVO	DATA	Redatto da RSGSI Firma	Approvato da AD
00	Prima Emissione			
02	Revisione Generale	01.08.2025		

1.0 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce la politica aziendale definita dalla Direzione di PLURIMA S.P.A. relativamente al Sistema di Gestione Sicurezza delle Informazioni (e sue estensioni per la Sicurezza del Cloud) e la Continuità Operativa.

La Politica ha carattere generale ed intende esprimere la volontà della Direzione aziendale di:

- accrescere la soddisfazione del Cliente;
- garantire la qualità, sicurezza delle informazioni, continuità operativa, gestione efficace nella fornitura dei propri prodotti e nell'erogazione dei propri servizi e tutela dell'ambiente;
- perseguire il miglioramento continuo di tutti i processi aziendali e servizi erogati con riguardo alle necessità e aspettative di tutte le parti interessate.

La Politica del Sistema di Gestione della Sicurezza delle Informazioni si applica a tutti i livelli e a tutte le attività svolte da PLURIMA S.P.A. ed in particolare all'attività oggetto di certificazione.

La seguente politica, e le politiche aziendali derivanti da essa, viene rivista in caso di cambiamenti significativi o almeno una volta all'anno in occasione del riesame della Direzione eventualmente confermandone la validità.

2.0 NORME DI RIFERIMENTO

- ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti ISO/IEC 27017:2021– Codice di pratica per i controlli di sicurezza delle informazioni basati su ISO / IEC 27002 per i servizi cloud
- ISO/IEC 27018:2020 – Codice di pratica per la protezione delle informazioni personali (PII) in cloud pubblici che agiscono come processori PII
- ISO/IEC 27035:2023 –Tecnologia dell'informazione – Gestione degli incidenti di sicurezza informatica
- ISO 22301:2019 – Sicurezza e resilienza – Sistemi di gestione per la continuità operativa – Requisiti
- ISO/IEC 20000-1:2018 – Tecnologia per l'informazione – Gestione dei servizi – Parte 1: Requisiti per il sistema di gestione dei servizi
- GDPR (Reg. UE 679/2016 e legislazione nazionale – D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i.)

3.0 PRINCIPI DELLA POLITICA DEL SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI

3.1 MOTIVAZIONE

PLURIMA S.P.A. percepisce la crescita aziendale come necessità per una maggiore diffusione della cultura della soddisfazione del cliente, della sicurezza delle informazioni e dell'erogazione dei propri servizi in maniera continuativa, efficiente. A tale scopo, ha assunto un ruolo attivo e operativo nelle attività di

impostazione e implementazione di:

- un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) secondo la ISO/IEC 27001 e le sue estensioni 27017 - 27018, anche a supporto della protezione dei dati personali secondo il regolamento europeo GDPR;

Data la natura delle proprie attività, PLURIMA S.p.A. considera, relativamente alla "**Gestione della Sicurezza delle Informazioni**", la qualità e la sicurezza delle informazioni fattori irrinunciabili per il miglioramento continuo delle prestazioni rese al Cliente, nell'ottica della sua soddisfazione e per la protezione del proprio patrimonio informativo, con l'obiettivo di aumentare la propria competitività sul mercato attraverso l'ottimizzazione dei propri processi progettuali, produttivi ed organizzativi.

PLURIMA S.p.A. pone particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di sviluppo e realizzazione dei propri servizi e prodotti, che devono essere ritenuti un bene primario dell'azienda.

I principi di sicurezza delle informazioni si applicano a tutte le attività e ed i servizi erogati ed ai dati ad esse collegati.

Consapevole del fatto che i propri servizi per soggetti esterni possono comportare l'affidamento di dati e informazioni critiche, l'organizzazione opera secondo normative di sicurezza internazionalmente riconosciute. Per questo motivo l'Azienda adotta le misure, sia tecniche che organizzative, necessarie a garantire al meglio la **Riservatezza, l'integrità e la disponibilità** del patrimonio informativo interno (informazioni e asset) e di quello affidatole dai propri Clienti tutelando- lo e proteggendolo da tutte le minacce, interne ed esterne, intenzionali o accidentali, nell'ambito delle proprie attività.

Con l'affidamento dei dati in cloud, PLURIMA S.p.A. ha adottato l'implementazione degli standard:

- ISO/IEC 27018 che riguarda la gestione dei dati personali in relazione alle soluzioni cloud. La gestione dei dati personali trattati all'interno dei nostri servizi cloud è soggetta a valutazione di parte terza nei suoi aspetti tecnici, organizzativi e contrattuali;
- ISO/IEC 27017 che definisce controlli di sicurezza supplementari e rinforzati per indirizzare le misure di sicurezza messe in atto dai provider di servizi Cloud. Si attesta quindi, con valutazione di parte terza, che tali controlli sono stati integrati all'interno del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI.

L'Azienda considera come ulteriori fattori determinanti per assicurare la qualità dei servizi offerti e la protezione delle informazioni, la capacità di adottare un approccio resiliente in situazioni di crisi che garantisca la continuità dell'operatività in sicurezza e la capacità di pianificazione e controllo dei servizi offerti che garantisca il soddisfacimento delle aspettative dei Clienti in maniera efficiente. I clienti dovrebbero valutare attentamente i servizi che scelgono in quanto le loro responsabilità varieranno in funzione dei servizi usati, dell'integrazione di quei servizi nel loro ambiente IT e delle leggi e normative applica.

3.2 OBIETTIVI

L'obiettivo del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI di **PLURIMA S.p.A.** è quello di garantire la sicurezza delle informazioni, la qualità, continuità ed efficienza dei servizi offerti attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali le informazioni ed i servizi stessi sono soggetti e attraverso un'adeguata comunicazione e continua formazione sulle tematiche relative al SGI che alimenti la consapevolezza, sensibilità e competenza dei propri dipendenti.

In particolare:

- Nell'ambito Sicurezza delle Informazioni ha l'obiettivo di:
 - Proteggere al meglio il patrimonio informativo proprio e dei propri Clienti, mediante l'implementazione di opportune misure organizzative, tecniche e procedurali per:
 - salvaguardare la RISERVATEZZA delle informazioni da accessi non autorizzati, stabilendo requisiti per l'accesso e relative modalità di assegnazione dei privilegi, sia per l'accesso logico che fisico alle informazioni o agli asset aziendali;
 - assicurare l'INTEGRITÀ delle informazioni, in modo che sia modificabile solo ed esclusivamente da chi ne possiede i privilegi;
 - garantire la DISPONIBILITÀ delle informazioni agli utenti autorizzati quando ne hanno bisogno, tramite la predisposizione di sistemi di backup delle informazioni uniformemente gestiti e monitorati e la redazione di piani per la continuità dell'attività aziendale opportunamente aggiornati, controllati e migliorati;
 - Assicurare la protezione dei dati personali nel rispetto dei principi e dei requisiti espressi dal GDPR, attuando misure adeguate ed efficaci che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche;
 - Definire e documentare una procedura per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione, in particolar modo quando questi coinvolgano dati personali (Data Breach) con una chiara indicazione dei ruoli e delle azioni correttive da intraprendere;
- Nell'ambito dell'erogazione di Servizi Cloud (Provider) ISO/IEC 27017:
 - Definire e mantenere sotto controllo:
 - le modalità di erogazione dei servizi cloud;
 - la gestione degli accessi ai servizi erogati in modalità cloud, secondo la politica di gestione degli accessi;
 - le comunicazioni ai Clienti in caso di change e agli interessati in caso di data breach;
 - il ciclo di vita degli account relativi ai servizi cloud;
 - l'esecuzione dell'analisi dei rischi derivanti dall'erogazione di un servizio cloud;
 - l'applicazione dei requisiti cogenti derivati dal Regolamento Europeo per la Protezione dei Dati Personali (GDPR).

- nell'ambito della fruizione di Servizi Cloud (Customer) ISO/IEC 27018:
 - Definire e mantenere sotto controllo:
 - le modalità di conservazione e accesso alle informazioni in cloud da parte del cloud service provider;
 - se e come viene effettuato il mantenimento in ambienti multi-tenant in cloud;
 - gli utenti che fruiscono dei servizi cloud e il contesto in cui li usano;
 - gli utenti amministratori dei servizi cloud fruiti in modalità customer, dotati di accessi privilegiati;
 - la localizzazione geografica dei provider di servizi cloud e i paesi in cui il provider può conservare i dati di PLURIMA S.P.A., anche temporaneamente.

3.3 ANALISI DEI RISCHI

Tutte le informazioni, che vengono create o utilizzate da PLURIMA S.P.A., sono da salvaguardare e devono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni devono essere gestite in modo sicuro, accurato e affidabile, e devono essere prontamente disponibili per gli usi consentiti.

Con "utilizzo dell'informazione" è da intendersi qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

Relativamente all'ambito di applicazione, in conformità alle norme ISO/IEC 27001:2022, ISO/IEC 27017:2021, ISO/IEC 27018:2020, il Responsabile per la Sicurezza delle Informazioni (RSGI) svolge periodicamente un'analisi dei rischi, con lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate, che tenga in considerazione gli obiettivi strategici espressi nella presente politica, gli incidenti occorsi durante tale periodo ed i cambiamenti strategici, di business e tecnologici avvenuti.

La Direzione condivide con il Responsabile per la Sicurezza delle Informazioni (RSGI) la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella redazione della metodologia la Direzione partecipa anche alla definizione delle scale di valore da impiegare per valorizzare i parametri che concorrono alla valutazione del rischio.

In seguito dell'elaborazione dell'analisi dei rischi da parte del Responsabile per la Sicurezza delle Informazioni (RSGI) ed in base alla metodologia condivisa con la Direzione, la Direzione stessa valuta i risultati ottenuti considerando la soglia di rischio accettabile, il trattamento di mitigazione dei rischi oltre tale soglia e il rischio residuo in seguito al trattamento.

L'analisi identifica chiaramente le azioni da intraprendere definendo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti.

L'analisi viene aggiornata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

3.4 REQUISITI

Accettazione della politica: tutti i dipendenti, collaboratori, fornitori, partner e tutte le altre parti interessate coinvolti nelle attività di PLURIMA S.p.A. devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse di PLURIMA S.p.A. o affidati a PLURIMA S.p.A. da terzi.

Asset aziendali: PLURIMA S.p.A. ha inventariato e mantiene costantemente aggiornato l'elenco degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno ha individuato un responsabile.

Classificazione: le informazioni gestite dall'azienda sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti ed appropriati; la classificazione risulta ad oggi di tipo Pubblica o Riservata. Ad esempio, tra i documenti del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI sono presenti documenti sia pubblici (Campo di applicazione), sia riservati (le procedure).

Accesso: l'accesso alle informazioni, ai beni e alle risorse di PLURIMA S.p.A. o affidati a PLURIMA S.p.A. da terzi, devono essere controllati e monitorati sulla base dei seguenti criteri:

- l'accesso è autorizzato solo per le informazioni strettamente necessarie (principio di conoscenza minima);
- l'accesso è autorizzato solo per le informazioni riguardanti le specifiche attività nelle quali si è coinvolti.

Consapevolezza: la Direzione aziendale assicura che ogni dipendente, collaboratore, fornitore o parte interessata sia consapevole, attui comportamenti ed utilizzi strumenti adeguati e in linea con la presente Politica.

Formazione: la Direzione aziendale garantisce che ogni risorsa sia addestrata/formata/informata sulle politiche organizzative applicate e sulle procedure relative al SGI.

Conformità normativa e legislativa: tutti i trattamenti delle informazioni e le procedure di **Plurima S.p.A.** sono conformi alle normative, alle leggi e ai regolamenti cogenti ed ai requisiti dei Clienti. PLURIMA S.p.A. tutela i dati personali in accordo al vigente Regolamento Privacy REG. UE 679/2016 e D. Lgs. 196/2003 aggiornato dal D. Lgs. 101/2018 e s.m.i. e provvedimenti del Garante Privacy, al CCNL applicabile, allo Statuto dei Lavoratori, agli accordi contrattuali con i collaboratori.

Protezione: tutte le informazioni, beni e risorse di PLURIMA S.p.A. o affidate a PLURIMA S.p.A. da parti terze sono protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in conformità con le leggi vigenti e in proporzione al loro valore. Le registrazioni rilevanti sono protette da perdita, distruzione, falsificazione, accessi e divulgazione non autorizzati, in conformità con i requisiti legali, normativi, contrattuali e di business, attraverso appositi strumenti tecnici, politiche specifiche e procedure operative cui si rimanda e descritte nel SGI.

Sicurezza nella progettazione e sviluppo: PLURIMA S.p.A. adotta un insieme di strumenti descritti nel SGI per garantire la sicurezza del processo di sviluppo, al fine di assicurare la riservatezza, l'integrità e la disponibilità delle soluzioni realizzate nell'ambito di tale processo.

Sicurezza del cloud: PLURIMA S.p.A. consente ai clienti di definire, eseguire e sfruttare il suo ambiente di sicurezza, avendo sviluppato un programma di controlli di sicurezza che implementa best practices di protezione della privacy (ISO/IEC 27018) e dati di livello globale (ISO/IEC 27017). Queste procedure di sicurezza e controllo sono convalidate in modo indipendente tramite valutazioni di terze parti. Il programma di controlli si basa sulla verifica, la dimostrazione e il monito- raggio.

Relazioni con parti terze: PLURIMA S.p.A. adotta la politica di responsabilizzare i propri fornitori e parti terze con cui collabora per le proprie attività, mediante specifici accordi di riservatezza e service level agreement / accordi sul livello del servizio (SLA); i suddetti accordi sono rivisti periodica- mente e comunque in occasione di ogni revisione della valutazione dei rischi.

Riesame della politica: l'approccio di PLURIMA S.p.A. nella gestione del SGI e della sua implementazione (requisiti, controlli, politiche, processi e procedure) viene rivisto nel periodico riesame della Direzione, o in modo indipendente dalla periodicità, quando intervengono cambiamenti significativi.

Costi: PLURIMA S.p.A. nell'attuare quanto precedentemente definito, valuta le spese necessarie per l'attuazione delle misure al fine di: proteggere le informazioni, i beni e le risorse dall'utilizzo non autorizzato, modifiche o distruzione; assicurare la continuità dei propri servizi critici a fronte di eventi imprevisti; garantire il rispetto dell'ambiente, degli SLA e della soddisfazione del Cliente nell'erogazione dei propri servizi.

4.0 RESPONSABILITÀ PER L'APPLICAZIONE DELLA POLITICA

La Direzione ha stabilito in maniera chiara e puntuale la presente Politica attraverso la definizione della propria strategia e degli obiettivi da perseguire.

La Direzione diffonde la presente Politica a tutti i livelli in modo che sia comunicata, compresa ed applicata, per ottenere l'adesione di tutti gli addetti e la loro collaborazione per il raggiungimento degli obiettivi stabiliti.

4.1 IMPEGNO DELLA DIREZIONE (DIR)

La Direzione di PLURIMA S.p.A. ha definito, divulgato, comunicato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente Politica del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI.

L'impegno della Direzione si attua tramite una struttura i cui compiti sono:

- definire ed approvare la Politica del Sistema SICUREZZA DELLE INFORMAZIONI;
- garantire che siano identificati tutti gli obiettivi relativi alla qualità, sicurezza delle informa- zioni, continuità operativa, gestione dei servizi e tutela dell'ambiente e che questi soddisfino i requisiti

aziendali;

- raggiungere il soddisfacimento dei Clienti offrendo prodotti e servizi efficienti ed in linea con le loro esigenze;
- introdurre una maggiore flessibilità nella propria organizzazione, atta ad individuare le cause dei problemi adottando tempestivamente i provvedimenti necessari alla loro risoluzione;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGI;
- fornire risorse sufficienti e adeguate alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;
- controllare che il SGI SICUREZZA DELLE INFORMAZIONI in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- fornire prodotti e servizi che soddisfino i requisiti del cliente, nel rispetto delle leggi, regolamenti e normative applicabili;
- privilegiare rapporti con fornitori che abbiano politiche di rispetto ambientale, accrescendo la qualità della relazione in un rapporto di reciproco beneficio;
- garantire la congruità dei budget destinati al raggiungimento degli obiettivi prefissati, coerentemente con le politiche e le linee strategiche aziendali definite;
- monitorare i cambiamenti dell'esposizione alle minacce dell'azienda, analizzare gli incidenti alla sicurezza, alla continuità ed ai servizi rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- sostenere tutte le iniziative inerenti al rispetto dell'ambiente e lo sviluppo sostenibile;
- attivare programmi per la diffusione della consapevolezza e della cultura della qualità, sicurezza delle informazioni, continuità ed efficienza dei servizi erogati e tutela dell'ambiente.

4.2 IMPEGNO DEL RESPONSABILE DEL SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI (RSGI)

Nell'ambito del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI e attraverso norme e procedure appropriate ed approvate, deve:

- effettuare l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio;
- definire tutti i requisiti cogenti (le norme, le leggi, i regolamenti, inclusi i requisiti specifici del cliente) necessari alla gestione di tutte le attività aziendali;
- verificare le violazioni alla presente Politica e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce;
- suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne il Sistema SICUREZZA DELLE INFORMAZIONI;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI.

4.3 IMPEGNO DI TUTTO IL PERSONALE

Tutto il personale (dipendente e collaboratore), qualunque sia il ruolo e/o la mansione svolta, è invitato ad attuare quanto indicato:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di PLURIMA S.p.A. o affidate a PLURIMA S.p.A. da terze parti;
- proteggere i beni e le risorse materiali, i sistemi informatici di PLURIMA S.p.A. o affidati a PLURIMA S.p.A. da terze parti;
- attuare un comportamento responsabile nei confronti dell'ambiente;
- informare la Direzione ovvero il RSGI, le autorità competenti in caso di accertate e/o presunte violazioni o rilevazione di tentate violazioni;
- informare la Direzione ovvero il RSGI, in caso si ritenga necessario apportare modifiche alla presente Politica e/o ai documenti del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI.

4.4 SOGGETTI ESTERNI

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono garantire il rispetto dei requisiti contenuti nella presente Politica.

I soggetti esterni coinvolti nel campo di applicazione del Sistema di Gestione SICUREZZA DELLE INFORMAZIONI e le linee guida di best practices sono i clienti e i fornitori, i collaboratori esterni (consulenti) operanti all'interno dell'azienda, che sono assimilabili ai dipendenti e che sottoscrivono una lettera di impegno di riservatezza.

Corciano(PE) 01.08.2025

La Direzione
