

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Sistema di Gestione per la Sicurezza delle Informazioni
conforme alla norma UNI CEI EN ISO/IEC 27001



Rev. 1 del 20/03/2026



01

Scopo e Campo di Applicazione

03

Obiettivi Strategici della Sicurezza

05

Ruoli e Responsabilità

07

Conformità Normativa e Requisiti Legali

09

Gestione degli Incidenti di Sicurezza

11

Approvazione della Direzione

02

La Triade CIA — Riservatezza, Integrità, Disponibilità

04

Impegno della Direzione

06

Gestione dei Rischi

08

Formazione e Sensibilizzazione

10

Miglioramento Continuo e Revisione

SCOPO

La presente Politica definisce gli obiettivi, i principi e le responsabilità in materia di sicurezza delle informazioni per BLUCLAD SPA, in conformità alla norma UNI CEI EN ISO/IEC 27001:2022.

Essa si applica a tutte le informazioni trattate dall'organizzazione — in qualunque forma esse si presentino (digitale, cartacea, verbale) — nonché a tutti i sistemi, processi e attività che le supportano.

CAMPO DI APPLICAZIONE

- Tutti i dipendenti, collaboratori e consulenti
- Tutti i sistemi informativi e le infrastrutture IT
- I dati e le informazioni di clienti e partner
- I servizi erogati e i relativi processi di supporto
- I fornitori che accedono ai sistemi aziendali
- Le sedi fisiche e i locali tecnici dell'azienda



RISERVATEZZA

Le informazioni sono accessibili esclusivamente a soggetti autorizzati. BLUCLAD SPA garantisce che i dati siano protetti da accessi non autorizzati mediante controlli di accesso, crittografia e politiche di classificazione delle informazioni.



INTEGRITÀ

Le informazioni sono accurate, complete e non alterate in modo non autorizzato. L'organizzazione adotta misure tecniche e procedurali per prevenire modifiche indebite e garantire l'autenticità dei dati lungo tutto il loro ciclo di vita.



DISPONIBILITÀ

Le informazioni sono accessibili e utilizzabili quando necessario da parte degli utenti autorizzati. BLUCLAD SPA assicura la continuità dei servizi mediante piani di backup, disaster recovery e gestione della continuità operativa.

01

Soddisfazione del cliente

Monitorare e identificare le esigenze dei clienti, offrendo soluzioni adeguate nel rispetto della riservatezza e integrità dei loro dati.

02

Eccellenza nell'erogazione dei servizi

Garantire i massimi standard di sicurezza nelle fasi di progettazione, erogazione e manutenzione dei servizi.

03

Competenza e formazione del personale

Assicurare adeguata selezione, formazione continua e sensibilizzazione di tutto il personale sulle tematiche di sicurezza.

04

Efficienza delle risorse

Utilizzare in modo efficace ed efficiente le risorse interne, rispettando le tempistiche dei clienti e gli impegni contrattuali.

05

Aggiornamento tecnologico

Monitorare costantemente l'evoluzione tecnologica e le novità del mercato, con attenzione agli aspetti di sicurezza delle informazioni.

06

Gestione proattiva dei rischi

Identificare, valutare e trattare i rischi per la sicurezza delle informazioni in modo sistematico e documentato.

La Direzione di BLUCLAD SPA si impegna formalmente a supportare, sviluppare e migliorare continuamente il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), garantendo le risorse necessarie e promuovendo una cultura della sicurezza a tutti i livelli organizzativi.

- 1 Garantire la conformità a tutti i requisiti cogenti, normativi e contrattuali applicabili ai servizi erogati.
- 2 Permettere il monitoraggio continuo delle attività per prevenire problemi e fornire alla direzione elementi concreti per la definizione degli obiettivi.
- 3 Assicurare che l'attenzione di tutto il personale sia rivolta al rispetto costante di riservatezza, integrità e disponibilità dei dati presenti in BLUCLAD.
- 4 Mettere a disposizione adeguati strumenti per il miglioramento continuo attraverso l'analisi e il monitoraggio delle tecnologie e dell'infrastruttura aziendale.
- 5 Comunicare l'importanza della sicurezza delle informazioni e le aspettative legate ai ruoli e responsabilità a tutti i membri dell'organizzazione.
- 6 Promuovere il miglioramento continuo del SGSI attraverso riesami periodici, audit interni e gestione strutturata delle non conformità.

Alta Direzione

- Approvazione e revisione della presente Politica
- Allocazione delle risorse per il SGSI
- Promozione della cultura della sicurezza

Responsabile SGSI (CISO)

- Coordinamento e supervisione del SGSI
- Gestione della valutazione dei rischi
- Reporting alla direzione sullo stato del SGSI

Responsabili di Processo

- Applicazione delle misure di sicurezza nel proprio ambito
- Segnalazione di incidenti e non conformità
- Partecipazione alle attività di audit interno

Tutto il Personale e Collaboratori

- Rispetto della presente Politica e delle procedure correlate
- Segnalazione di incidenti o comportamenti anomali
- Partecipazione ai programmi di formazione obbligatori

1

Identificazione

Individuazione degli asset informativi e delle minacce/vulnerabilità associate

2

Valutazione

Analisi della probabilità e dell'impatto potenziale di ciascun rischio identificato

3

Trattamento

Selezione delle misure di controllo (mitigazione, accettazione, trasferimento, eliminazione)

4

Monitoraggio

Verifica continua dell'efficacia dei controlli implementati e degli indicatori di rischio

5

Riesame

Revisione periodica del processo di risk assessment in occasione di variazioni significative

La valutazione dei rischi viene effettuata almeno annualmente, in occasione di variazioni significative al contesto organizzativo o tecnologico, e documentata nell'Analisi dei rischi V.E.R.A.. I criteri di accettazione del rischio sono definiti e approvati dalla Direzione.

ISO/IEC 27001:2022

Standard internazionale per i Sistemi di Gestione della Sicurezza delle Informazioni

D.Lgs. 196/2003 (Codice Privacy)

Normativa italiana in materia di protezione dei dati personali, aggiornata con D.Lgs. 101/2018

Requisiti contrattuali

Obblighi di riservatezza e sicurezza presenti nei contratti con clienti e fornitori

GDPR (Reg. UE 2016/679)

Regolamento generale europeo sulla protezione dei dati personali

Direttiva NIS2 (UE 2022/2555)

Misure per un elevato livello comune di sicurezza informatica nell'UE

Norme tecniche di settore

Standard e best practice specifici del settore di attività dell'organizzazione

BLUCLAD SPA mantiene aggiornato un registro delle normative applicabili e verifica periodicamente la propria conformità attraverso audit interni e riesami della direzione.

PROGRAMMA DI FORMAZIONE

- Formazione obbligatoria iniziale per tutti i nuovi assunti
- Aggiornamento annuale su politiche e procedure di sicurezza
- Formazione specialistica per ruoli con accesso a dati sensibili
- Simulazioni di phishing e social engineering
- Esercitazioni su scenari di incidente informatico
- Comunicazioni periodiche su minacce emergenti

Consapevolezza

Ogni membro dell'organizzazione deve essere consapevole della propria responsabilità nella protezione delle informazioni aziendali e delle conseguenze di comportamenti non conformi.

Registrazione

Tutte le attività di formazione vengono registrate e tracciate. L'efficacia dei programmi formativi è verificata periodicamente dalla Direzione e dal Responsabile SGSI.

Conseguenze

Il mancato rispetto della presente Politica e delle procedure correlate può comportare azioni disciplinari, fino alla risoluzione del rapporto di lavoro o collaborazione.

BLUCLAD SPA adotta un processo strutturato per la gestione degli incidenti di sicurezza delle informazioni, garantendo una risposta tempestiva ed efficace per minimizzare l'impatto e prevenire il ripetersi degli eventi.

1

Rilevazione e Segnalazione

Chiunque rilevi o sospetti un incidente di sicurezza è tenuto a segnalarlo immediatamente al Responsabile SGSI attraverso i canali dedicati.

2

Valutazione e Classificazione

Il Responsabile SGSI valuta la gravità dell'incidente, ne classifica il tipo e attiva le procedure di risposta appropriate in base al livello di severità.

3

Contenimento e Risposta

Vengono adottate misure immediate per contenere l'incidente, ridurre l'impatto, preservare le prove e ripristinare le normali condizioni operative.

4

Analisi Post-Incidente

Al termine di ogni incidente significativo viene condotta un'analisi delle cause radice per migliorare i controlli e prevenire il verificarsi di eventi analoghi.

Gli incidenti che coinvolgono dati personali sono notificati al Garante Privacy entro 72 ore ai sensi dell'art. 33 GDPR.

Gli incidenti che rientrano nel perimetro NIS2 sono presi in carico e comunicati sulla piattaforma CSIRT come previsto dalla procedura di incident management.

CICLO DI REVISIONE

Cadenza annuale

Revisione ordinaria programmata dalla Direzione

Variazioni organizzative

Cambiamenti significativi a struttura, servizi o processi

Incidenti rilevanti

A seguito di incidenti di sicurezza di particolare gravità

Nuovi requisiti normativi

Introduzione di nuove leggi, regolamenti o standard

Risultati di audit

Non conformità emerse da audit interni o di terza parte

Variazioni al contesto

Nuove minacce, tecnologie o mutamenti del mercato

CICLO PDCA — MIGLIORAMENTO CONTINUO



PLAN

Pianificazione obiettivi, valutazione rischi, definizione controlli



DO

Implementazione dei controlli e delle procedure di sicurezza



CHECK

Monitoraggio, misurazione, audit interni, riesame della direzione



ACT

Azioni correttive, miglioramento continuo del SGSI

APPROVAZIONE DELLA DIREZIONE

La presente Politica della Sicurezza delle Informazioni è stata approvata dall'Alta Direzione di BLUCLAD SPA ed è vincolante per tutti i dipendenti, collaboratori e fornitori che operano per conto dell'organizzazione.

FIRMA DELL'AMMINISTRATORE DELEGATO



Firma e timbro

Nome e Cognome: LORENZO CAVACIOCCHI

INFORMAZIONI DOCUMENTO

Versione:	Rev. 1
Data di emissione:	20/03/2026
Prossima revisione:	20/03/2027
Classificazione:	OPEN
Standard di rif.:	ISO/IEC 27001:2022