

POL Politica di sicurezza delle informazioni

Nome della società	CAST INFORMATICA S.r.l.
Data di entrata in vigore	19/09/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	19/09/2025	-- N/D --	Andrea Coppola	Andrea Coppola

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

- Campo di Applicazione
- Riferimenti Normativi
- Termini e Definizioni
- Ruoli e Responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Archiviazione e Aggiornamenti
- Documenti di Riferimento

Campo di Applicazione

La presente politica definisce i principi, gli obiettivi e le direttive generali per la gestione della sicurezza delle informazioni all'interno di CAST INFORMATICA S.r.l. Il suo scopo è proteggere il patrimonio informativo aziendale e quello dei clienti da minacce interne ed esterne, garantendo la continuità operativa e la conformità ai requisiti normativi e contrattuali. Questa politica si applica a tutto il personale, ai processi, alle tecnologie e alle informazioni gestite nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Riferimenti Normativi

- ISO/IEC 27001
- ISO/IEC 27017
- Regolamento (UE) 2016/679 (GDPR)

Termini e Definizioni

- **Riservatezza** : Proprietà che assicura che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : Proprietà relativa all'accuratezza e alla completezza delle informazioni e degli asset.
- **Disponibilità** : Proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

Ruoli e Responsabilità

- **Titolare** : Definisce la direzione strategica e gli obiettivi per la sicurezza delle informazioni, approva la relativa politica, assicura l'allocazione delle risorse necessarie per la sua attuazione e ne promuove la cultura a livello aziendale.
- **Responsabile del sistema di gestione integrato (RSGI)** : Supervisiona lo sviluppo, l'implementazione e il mantenimento del Sistema di Gestione della Sicurezza delle Informazioni (SGSI). È responsabile della gestione dei rischi, del coordinamento degli audit, della supervisione della risposta agli incidenti e della comunicazione della documentazione pertinente.
- **Sistemista** : Implementa, gestisce e mantiene le configurazioni di sicurezza per i sistemi IT, le reti e gli ambienti cloud. È responsabile dell'applicazione delle patch di sicurezza, della risposta tecnica agli incidenti e della gestione delle procedure di backup e ripristino.
- **Tecnici Onsite** : Aderiscono alle politiche di sicurezza durante gli interventi presso i clienti, garantendo la gestione sicura dei dispositivi e dei dati a cui accedono e segnalando eventuali anomalie o incidenti di sicurezza.

Obiettivi di sicurezza delle informazioni

CAST INFORMATICA S.r.l. si impegna a proteggere il proprio patrimonio informativo e quello dei suoi clienti da ogni minaccia, interna o esterna, intenzionale o accidentale. La Direzione, nella persona del **Titolare**, definisce e promuove gli obiettivi strategici per la sicurezza delle informazioni, in linea con il contesto e il business aziendale.

Gli obiettivi primari del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sono:

- **Riservatezza** : Garantire che le informazioni siano accessibili esclusivamente al personale e alle parti interessate autorizzate.
- **Integrità** : Salvaguardare l'accuratezza, la completezza e la validità delle informazioni e dei metodi di elaborazione, proteggendole da modifiche non autorizzate.
- **Disponibilità** : Assicurare che il personale autorizzato e i clienti possano accedere alle informazioni e agli asset associati quando necessario, garantendo la continuità dei servizi erogati.

Per raggiungere tali obiettivi, CAST INFORMATICA S.r.l. si impegna a:

- Implementare e mantenere un Sistema di Gestione della Sicurezza delle Informazioni conforme allo standard ISO/IEC 27001.
- Assicurare la conformità con i requisiti legali, normativi e contrattuali applicabili, inclusi quelli relativi alla protezione dei dati personali.
- Adottare un approccio basato sulla valutazione e sul trattamento del rischio per orientare le decisioni in materia di sicurezza.
- Promuovere una cultura della sicurezza a tutti i livelli dell'organizzazione, aumentando la consapevolezza e la competenza del personale.
- Perseguire il miglioramento continuo delle prestazioni del SGSI.

La pianificazione, l'attuazione e il monitoraggio di obiettivi specifici e misurabili sono gestiti in conformità alla procedura "PRO Obiettivi e pianificazione per il loro raggiungimento".

Principi fondamentali di sicurezza delle informazioni

Gestione e Revisione del SGSI

La presente politica e le politiche specifiche che ne derivano sono approvate dal **Titolare**, che ne assume la responsabilità ultima. Il **Responsabile del sistema di gestione integrato (RSGI)** ha il compito di mantenere, riesaminare e comunicare la documentazione del SGSI a tutto il personale e alle parti interessate rilevanti. La revisione della politica è condotta con cadenza almeno annuale e ogni qualvolta si verifichino cambiamenti significativi, come formalizzato nella procedura "PRO Gestione riesame della direzione".

Ruoli e Responsabilità

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge tutto il personale. Il **Titolare** detiene la responsabilità finale per la sicurezza delle informazioni, mentre il **Responsabile del sistema di gestione integrato (RSGI)** supervisiona l'implementazione e il mantenimento del SGSI. Ruoli e responsabilità specifici sono definiti e assegnati formalmente tramite la "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e la "PRO Procedura dei ruoli e responsabilità".

Uso Accettabile delle Risorse

Tutti gli asset informativi, inclusi hardware, software, dati e reti, devono essere utilizzati esclusivamente per scopi aziendali autorizzati e in conformità con quanto stabilito nel "Codice di condotta". L'accesso alle informazioni è regolato dal principio del minimo privilegio e gestito dal **Responsabile del sistema di gestione integrato (RSGI)** in accordo con la "PRO Procedura di gestione e controllo degli accessi logici".

Sicurezza nell'Uso dei Servizi Cloud

CAST INFORMATICA S.r.l., agendo sia come cliente sia come fornitore di servizi cloud, adotta principi specifici per la gestione della sicurezza in tali ambienti, come dettagliato nella "POL Politica di sicurezza del cloud".

- **Come Cliente di Servizi Cloud** : La selezione e la gestione dei fornitori di servizi cloud sono subordinate a una valutazione dei rischi e dei livelli di sicurezza offerti. Tale processo è governato dalla "PRO Procedura di gestione degli acquisti e delle terze parti" sotto la supervisione del **Responsabile del sistema di gestione integrato (RSGI)** .
- **Come Fornitore di Servizi Cloud** : CAST INFORMATICA S.r.l. deve garantire la sicurezza dei servizi erogati ai propri clienti, implementando controlli adeguati per l'isolamento tra i clienti (multi-tenancy), la sicurezza della virtualizzazione e la protezione dei dati dei clienti. Il **Sistemista** è responsabile dell'implementazione delle configurazioni sicure.

Protezione degli Asset Aziendali

Tutto il personale è tenuto a proteggere gli asset informativi e le risorse tecnologiche di CAST INFORMATICA S.r.l.

- **Scrivania Pulita e Schermo Pulito** : È fatto obbligo di non lasciare documenti contenenti informazioni sensibili incustoditi sulle postazioni di lavoro e di bloccare la propria sessione di lavoro quando ci si allontana. Il **Sistemista** deve configurare il blocco automatico dello schermo dopo un breve periodo di inattività, impostato a 5 minuti.
- **Asset Fuori Sede** : Gli asset aziendali, come i notebook assegnati ai **Tecnici Onsite** per interventi presso i clienti, devono essere protetti da furto, perdita o accesso non autorizzato quando si trovano all'esterno della sede aziendale. L'assegnazione e la responsabilità di tali beni sono formalizzate tramite il "MOD Modulo di assegnazione dei beni". La protezione degli asset è normata dalla "PRO Procedura di configurazione, gestione e smaltimento degli asset".

Segnalazione e Gestione degli Eventi di Sicurezza

Qualsiasi dipendente che osservi o sospetti un evento, un incidente o una vulnerabilità di sicurezza delle informazioni ha l'obbligo di segnalarlo tempestivamente al **Responsabile del sistema di gestione integrato (RSGI)** o al **Sistemista**. La gestione di tali eventi segue un processo strutturato definito nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni" e gli incidenti vengono tracciati nel "MOD Registro degli incidenti di sicurezza delle informazioni".

Archiviazione e Aggiornamenti

La presente politica è gestita in formato elettronico e archiviata all'interno del sistema documentale aziendale. Viene riesaminata con cadenza almeno annuale, e ogni qualvolta si verificano cambiamenti organizzativi, tecnologici o normativi significativi, per garantirne la continua idoneità, adeguatezza ed efficacia. Ogni aggiornamento è approvato dalla Direzione.

Documenti di Riferimento

- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Gestione riesame della direzione
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura dei ruoli e responsabilità
- Codice di condotta
- PRO Procedura di gestione e controllo degli accessi logici
- POL Politica di sicurezza del cloud
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- MOD Modulo di assegnazione dei beni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- MOD Registro degli incidenti di sicurezza delle informazioni