POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	24/11/2025	Angelica Scaglione	Marco Pellecchia

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

La presente politica definisce i principi e gli obiettivi strategici per la gestione della sicurezza delle informazioni all'interno di LINKINFORMATICA S.r.l. Lo scopo è proteggere il patrimonio informativo aziendale e quello dei clienti, in conformità con la missione aziendale di fornitore di soluzioni IT complete e affidabili. Questo documento si applica a tutti i processi, le risorse, i dipendenti e le terze parti che gestiscono informazioni per conto dell'azienda, costituendo il quadro di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Riferimenti normativi

- Direttiva (UE) 2022/2555 (Direttiva NIS 2)
- ISO/IEC 27001

Termini e definizioni

- **Bene (Asset)** : Qualsiasi cosa abbia un valore per l'organizzazione, includendo non solo oggetti fisici ma anche software, informazioni, persone e reputazione.
- **Riservatezza** : La proprietà che le informazioni non siano rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : La proprietà di salvaguardare l'accuratezza e la completezza dei beni.
- **Disponibilità** : La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Sicurezza delle informazioni** : La preservazione di riservatezza, integrità e disponibilità delle informazioni.
- **Incidente** : Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati, o dei servizi offerti o accessibili tramite sistemi informatici e di rete.

Ruoli e responsabilità

- **Amministratore Unico (CEO)** : Ha la responsabilità ultima della sicurezza delle informazioni, approva le politiche del SGSI e si impegna a fornire le risorse necessarie per il loro mantenimento e miglioramento.
- **Responsabile del Sistema di Gestione della Sicurezza** : Ha la responsabilità operativa di implementare, mantenere e migliorare il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità con le direttive aziendali e gli standard di riferimento.

Obiettivi di sicurezza delle informazioni

LINKINFORMATICA S.r.l. si impegna a proteggere il proprio patrimonio informativo e quello dei suoi clienti, in linea con la propria missione di fornitore di soluzioni IT complete e affidabili. Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conforme agli standard ISO/IEC 27001 e alla direttiva NIS2, è lo strumento strategico per governare i rischi e garantire la resilienza operativa.

Gli obiettivi strategici che guidano la presente politica sono:

- **Riservatezza** : Assicurare che le informazioni siano accessibili esclusivamente al personale e alle parti interessate autorizzate, prevenendo divulgazioni o accessi non consentiti.
- **Integrità** : Salvaguardare l'accuratezza, la completezza e la validità delle informazioni e dei sistemi che le elaborano, proteggendole da modifiche, alterazioni o distruzioni improprie.
- **Disponibilità** : Garantire che le informazioni, i sistemi e i servizi IT siano sempre accessibili e utilizzabili quando necessario, assicurando la continuità operativa per l'azienda e per i servizi erogati ai clienti.
- **Conformità** : Rispettare tutti i requisiti legali, normativi (inclusa la direttiva NIS2), statutari e contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati.
- **Miglioramento Continuo** : Riesaminare e migliorare costantemente l'efficacia del SGSI attraverso il monitoraggio delle prestazioni, la gestione degli incidenti e la valutazione periodica dei rischi e delle opportunità.

L'Amministratore Unico (CEO) approva la presente politica e si impegna a fornire le risorse necessarie per il suo mantenimento e per il raggiungimento degli obiettivi prefissati. La politica viene riesaminata con cadenza almeno annuale, e ogni qualvolta si verifichino cambiamenti significativi, per garantirne la continua idoneità e adeguatezza.

Principi fondamentali di sicurezza delle informazioni

Tutte le attività di LINKINFORMATICA S.r.l. devono essere condotte nel rispetto dei seguenti principi fondamentali, che costituiscono la base per tutte le politiche specifiche e le procedure operative del SGSI.

Gestione del Rischio e Miglioramento Continuo

LINKINFORMATICA S.r.l. adotta un approccio alla gestione della sicurezza basato sul rischio.

- **Valutazione del Rischio** : L'organizzazione deve identificare, analizzare e valutare i rischi per la sicurezza delle informazioni in modo sistematico, al fine di implementare trattamenti adeguati. Tale processo è descritto nella "PRO Procedura di gestione dei rischi".
- **Miglioramento Continuo** : Il Responsabile del Sistema di Gestione della Sicurezza deve definire e attuare un piano per la valutazione periodica dell'efficacia delle misure di gestione del rischio. Sulla base dei risultati delle valutazioni, degli audit e dei riesami,

l'Amministratore Unico (CEO) deve approvare un piano di adeguamento per assicurare il miglioramento continuo del SGSI. L'Amministratore Unico (CEO) deve essere informato periodicamente sull'avanzamento di tali piani, come dettagliato nella "PRO Procedura delle misurazioni e del monitoraggio" e nella "PRO Gestione riesame della direzione".

Ruoli e Responsabilità

Le responsabilità per la sicurezza delle informazioni sono definite, assegnate e comunicate a tutti i livelli dell'organizzazione.

- **Definizione** : I ruoli e le responsabilità in materia di sicurezza sono formalizzati e mantenuti aggiornati, in coerenza con quanto definito nel "MOD Organigramma" e nei "MOD Mansionario". Le direttive specifiche sono contenute nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e nella "PRO Procedura dei ruoli e responsabilità".
- **Approvazione e Riesame** : L'organizzazione per la sicurezza, inclusi ruoli e responsabilità, è approvata dall'Amministratore Unico (CEO) e riesaminata almeno ogni due anni o a seguito di incidenti o cambiamenti organizzativi significativi.
- **Leadership** : L'Amministratore Unico (CEO) ha la responsabilità ultima della sicurezza delle informazioni e approva tutte le politiche del SGSI. Il Responsabile del Sistema di Gestione della Sicurezza ha la responsabilità operativa di implementare, mantenere e migliorare il SGSI.

Sicurezza delle Risorse Umane

La sicurezza delle informazioni è parte integrante del ciclo di vita del personale.

- **Selezione** : Il personale con accesso a sistemi e informazioni rilevanti, inclusi gli amministratori di sistema, deve essere individuato previa valutazione di esperienza, capacità e affidabilità, come specificato nella "PRO Procedura di gestione delle risorse umane".
- **Durante l'impiego** : Tutto il personale deve essere formato e sensibilizzato sui propri doveri in materia di sicurezza.
- **Cessazione del rapporto** : Alla cessazione o modifica del rapporto di lavoro, gli obblighi di riservatezza devono rimanere validi, come stabilito a livello contrattuale. La restituzione dei beni aziendali e la revoca degli accessi devono seguire un processo formale, come indicato nel "MOD Lista di controllo per uscita dei dipendenti".

Gestione degli Asset e Uso Accettabile

Tutti gli asset informativi e le risorse associate devono essere identificati, classificati e protetti adeguatamente.

- **Inventario e Classificazione** : Tutti gli asset devono essere censiti e classificati in base alla loro criticità, come descritto nella "PRO Procedura di configurazione, gestione e smaltimento degli asset".

- **Uso Accettabile** : Devono essere implementate regole chiare per l'uso accettabile delle informazioni e delle risorse aziendali, come computer, reti e software. Tali regole sono definite nel "Codice di condotta".
- **Protezione dei Beni** : I beni aziendali, inclusi quelli utilizzati fuori sede (lavoro da remoto), devono essere protetti da furto, danno o accesso non autorizzato. L'assegnazione e la restituzione dei beni sono formalizzate tramite il "MOD Modulo di assegnazione dei beni" e il "MOD Modulo di restituzione dei beni".
- **Scrivania e Schermo Puliti** : Devono essere applicate regole per la protezione di documenti cartacei, supporti di memorizzazione rimovibili e per le postazioni di lavoro incustodite, che prevedono il blocco automatico della sessione dopo un periodo di inattività.

Controllo degli Accessi

L'accesso alle informazioni e ai sistemi informativi deve essere controllato secondo i principi di minimo privilegio e separazione dei compiti.

- **Principi** : L'accesso è concesso solo sulla base di effettive necessità operative (need-to-know) e limitato alle sole informazioni e funzioni necessarie per svolgere il proprio ruolo.
- **Gestione** : Il ciclo di vita delle utenze (creazione, modifica, revoca) deve seguire un processo di autorizzazione formale, come dettagliato nella "PRO Procedura di gestione e controllo degli accessi logici".

Sicurezza Fisica e Ambientale

Le sedi aziendali e le aree che contengono informazioni o infrastrutture critiche devono essere protette da accessi non autorizzati, danni e interferenze. Le misure di protezione sono definite nella "PRO Procedura di sicurezza fisica e ambientale".

Sicurezza Operativa

L'integrità e la disponibilità dei sistemi e dei processi devono essere garantite attraverso controlli operativi robusti.

- **Gestione dei Cambiamenti** : Qualsiasi modifica all'infrastruttura, ai sistemi o ai processi deve essere valutata, autorizzata e documentata per gestirne gli impatti sulla sicurezza, come definito nella "PRO Procedura di gestione del cambiamento".
- **Protezione da Malware e Vulnerabilità** : Devono essere implementate misure per prevenire, rilevare e rimuovere software malevolo e per gestire le vulnerabilità tecniche dei sistemi.
- **Backup** : Le informazioni critiche devono essere sottoposte a backup regolari e testate per garantirne il ripristino, come specificato nella "POL Politica di sicurezza operativa".
- **Monitoraggio** : Le attività sui sistemi e sulle reti devono essere registrate e monitorate per rilevare eventi anomali o potenziali incidenti di sicurezza.

Sicurezza delle Comunicazioni e della Rete

Le reti e i flussi di informazioni devono essere protetti per prevenire accessi non autorizzati e garantire l'integrità dei dati in transito. Le misure di sicurezza, come la segmentazione della rete e la configurazione sicura dei dispositivi, sono definite nella "PRO Procedura di gestione della sicurezza della rete".

Sicurezza della Catena di Approvvigionamento

I rischi per la sicurezza derivanti dalla catena di approvvigionamento e dai rapporti con fornitori e partner devono essere identificati e gestiti.

- **Valutazione** : I fornitori che hanno accesso a informazioni o sistemi aziendali devono essere valutati in base ai loro standard di sicurezza.
- **Accordi Contrattuali** : I requisiti di sicurezza delle informazioni devono essere inclusi negli accordi contrattuali con i fornitori, come descritto nella "PRO Procedura di gestione degli acquisti e delle terze parti".

Gestione degli Incidenti di Sicurezza

L'organizzazione deve essere preparata a rispondere in modo tempestivo ed efficace agli incidenti di sicurezza.

- **Segnalazione** : Tutto il personale ha la responsabilità di segnalare immediatamente qualsiasi evento o debolezza di sicurezza osservata o sospetta attraverso i canali designati, come indicato nella "PRO Procedura di gestione dei rilievi ed eventi".
- **Risposta** : Deve essere implementato un processo formale per la gestione degli incidenti, che copra tutte le fasi dalla rilevazione alla risoluzione e all'analisi post-incidente, come dettagliato nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".

Continuità Operativa

LINKINFORMATICA S.r.l. deve garantire la capacità di continuare a operare e a erogare servizi critici a fronte di interruzioni significative. Le strategie e i piani per la continuità operativa e il ripristino di emergenza sono definiti nella "PRO Procedura di continuità operativa e di ripristino di emergenza".

Conformità

L'organizzazione deve garantire la conformità a tutti i requisiti legali, normativi e contrattuali pertinenti.

- **Requisiti** : I requisiti applicabili devono essere identificati, documentati e tenuti aggiornati.
- **Proprietà Intellettuale** : Deve essere garantito il rispetto delle licenze software e dei diritti di proprietà intellettuale.

- **Audit** : L'aderenza alle politiche e alle procedure di sicurezza deve essere verificata periodicamente attraverso audit interni ed esterni, gestiti secondo la "PRO Gestione audit interni".

Archiviazione e aggiornamenti

Questo documento è archiviato nel sistema di gestione documentale aziendale. Viene riesaminato con cadenza almeno annuale, o a seguito di cambiamenti organizzativi, tecnologici o normativi significativi, per assicurarne la continua idoneità, adeguatezza ed efficacia. L'aggiornamento è responsabilità del Responsabile del Sistema di Gestione della Sicurezza, con l'approvazione finale dell'Amministratore Unico (CEO).

Documenti di riferimento

- PRO Procedura di gestione dei rischi
- PRO Procedura delle misurazioni e del monitoraggio
- PRO Gestione riesame della direzione
- MOD Organigramma
- MOD Mansionario
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura dei ruoli e responsabilità
- PRO Procedura di gestione delle risorse umane
- MOD Lista di controllo per uscita dei dipendenti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- Codice di condotta
- MOD Modulo di assegnazione dei beni
- MOD Modulo di restituzione dei beni
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di gestione del cambiamento
- POL Politica di sicurezza operativa
- PRO Procedura di gestione della sicurezza della rete
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di gestione dei rilievi ed eventi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di continuità operativa e di ripristino di emergenza

- PRO Gestione audit interni