POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	20/10/2025	Fabrizio Sebastiani	Andrea Del Sole
2	17/04/2026	Fabrizio Sebastiani	Andrea Del Sole

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, gli obiettivi e le direttive generali per la gestione della sicurezza delle informazioni all'interno di Arakne S.r.l. Si applica a tutte le informazioni, i sistemi informativi, le reti, le applicazioni e le risorse tecnologiche gestite dall'azienda, nonché a tutto il personale, ai collaboratori e alle terze parti che hanno accesso agli asset informativi aziendali. Lo scopo è proteggere gli asset informativi da tutte le minacce, interne o esterne, deliberate o accidentali, in conformità con i requisiti di business, legali e normativi.

Riferimenti Normativi

- ISO/IEC 27001
- Direttiva (UE) 2022/2555 (NIS2)

Termini e Definizioni

- **Riservatezza** : Proprietà per cui le informazioni non vengono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : Proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Disponibilità** : Proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

Ruoli e Responsabilità

- **Direzione Aziendale (DA)** : Definisce e approva la politica e gli obiettivi strategici per la sicurezza delle informazioni, assicurando l'assegnazione delle risorse necessarie e riesaminando l'efficacia del Sistema di Gestione.
- **Responsabile del Sistema di Gestione Integrato (RSGI)** : Implementa, mantiene e migliora il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conduce l'analisi dei rischi e ne monitora il trattamento, assicurando la conformità agli standard di riferimento.
- **Responsabile della Cybersicurezza (RCYB)** : Definisce, implementa e mantiene la strategia di cybersicurezza aziendale, garantendo la protezione operativa degli asset informatici e coordinando le attività tecniche di sicurezza.
- **Punto di Contatto NIS2 (PCNIS2)** : Funge da punto di contatto ufficiale con le autorità competenti per gli adempimenti previsti dalla Direttiva NIS2, gestendo le comunicazioni e le notifiche obbligatorie.
- **Responsabile Sviluppo Risorse Umane (RU)** : Assicura che i processi di selezione, assunzione e cessazione del personale includano gli adempimenti necessari a garantire la sicurezza delle informazioni, come la firma di accordi di riservatezza.

- **Responsabile Ufficio Acquisti (RACQ)** : Gestisce il processo di approvvigionamento assicurando che i rischi per la sicurezza delle informazioni siano valutati e gestiti nei rapporti con i fornitori.
- **Responsabile Qualifica Fornitori (RQF)** : Conduce la valutazione e la qualifica dei fornitori, includendo la verifica dei loro requisiti di sicurezza delle informazioni.
- **Referente del Computer Security Incident Response Team (RCSIRT)** : Coordina la gestione operativa degli incidenti di sicurezza informatica, dalla rilevazione alla risoluzione, assicurando una risposta efficace e tempestiva.
- **Direttore Tecnico (DIRTEC)** : È responsabile della definizione e dell'attuazione dei piani di continuità operativa per garantire la resilienza dei servizi erogati.
- **Responsabile del Sistema Informativo (RSI)** : Gestisce l'infrastruttura tecnologica aziendale e partecipa alla definizione e all'implementazione dei piani di continuità operativa e di ripristino di emergenza.

Obiettivi di sicurezza delle informazioni

Arakne S.R.L. si impegna a proteggere i propri asset informativi, quelli dei suoi clienti e delle parti interessate, in linea con la propria missione aziendale di progettare e fornire soluzioni ICT innovative. La Direzione Aziendale (DA) definisce e approva gli obiettivi strategici per la sicurezza delle informazioni, assicurando che siano allineati al contesto organizzativo, ai requisiti legali e contrattuali, e riesaminati con cadenza almeno annuale durante il riesame della direzione.

Gli obiettivi strategici di sicurezza delle informazioni si fondano sui seguenti pilastri:

- **Riservatezza** : Garantire che le informazioni siano accessibili solo al personale autorizzato. Arakne si impegna a proteggere la proprietà intellettuale propria e dei clienti, i dati personali e le informazioni commerciali sensibili da accessi, utilizzi o divulgazioni non autorizzati.
- **Integrità** : Salvaguardare l'accuratezza, la completezza e la coerenza delle informazioni e dei sistemi che le elaborano. Arakne adotta misure per prevenire modifiche non autorizzate o accidentali ai dati durante il loro intero ciclo di vita.
- **Disponibilità** : Assicurare che le informazioni, i sistemi e le risorse necessarie per l'erogazione dei servizi siano sempre accessibili e utilizzabili quando richiesto dal personale e dai clienti, garantendo la continuità operativa.

Per il raggiungimento di tali obiettivi, la Direzione Aziendale (DA) si impegna a:

- Adottare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme a ISO/IEC 27001 e ai requisiti della Direttiva NIS2.
- Promuovere una cultura della sicurezza a tutti i livelli dell'organizzazione, basata sulla consapevolezza e sulla responsabilità individuale e collettiva.
- Assegnare risorse adeguate per l'implementazione, il mantenimento e il miglioramento continuo del SGSI.

- Definire e monitorare obiettivi misurabili per la sicurezza delle informazioni, come dettagliato nel documento **PRO Obiettivi e pianificazione per il loro raggiungimento** .

Principi fondamentali di sicurezza delle informazioni

Arakne S.R.L. stabilisce che la sicurezza delle informazioni è una responsabilità condivisa, guidata dalla **Direzione Aziendale (DA)** e attuata da tutto il personale. Tutti i processi, le policy e le procedure aziendali devono essere conformi ai seguenti principi fondamentali.

Gestione del Rischio e Miglioramento Continuo

Arakne adotta un approccio sistematico basato sul rischio per identificare, analizzare, valutare e trattare le minacce alla sicurezza delle informazioni. Il **Responsabile del Sistema di Gestione Integrato (RSGI)** ha la responsabilità di condurre il processo di valutazione del rischio, come definito nella **PRO Procedura di gestione dei rischi.** La **Direzione Aziendale (DA)** approva la strategia di trattamento del rischio e il piano di adeguamento. L'efficacia delle misure viene riesaminata periodicamente per garantire il miglioramento continuo del SGSI, in accordo con la **PRO Gestione riesame della direzione.**

Ruoli, Responsabilità e Governance

La **Direzione Aziendale (DA**) approva la struttura organizzativa per la sicurezza, definendo e assegnando ruoli e responsabilità in modo chiaro e documentato. Tali compiti sono formalizzati nel **MOD Ruoli Mansionario Responsabilita** e nella **POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni** . Il **Responsabile del Sistema di Gestione Integrato (RSGI**) è incaricato di implementare e mantenere il SGSI. Il Responsabile della Cybersicurezza (RCYB) definisce e mantiene la strategia di cybersicurezza. Il Punto di Contatto NIS2 (PCNIS2) e il suo sostituto sono formalmente designati per gestire le comunicazioni con le autorità competenti. I ruoli e le responsabilità vengono riesaminati almeno ogni due anni o a seguito di cambiamenti significativi.

Sicurezza delle Risorse Umane

Arakne garantisce che tutto il personale, inclusi i collaboratori, sia affidabile e consapevole delle proprie responsabilità in materia di sicurezza. Il **Responsabile Sviluppo Risorse Umane (RU)** assicura che il processo di selezione valuti l'esperienza e l'affidabilità dei candidati, in particolare per ruoli critici come gli amministratori di sistema. Tutti i contratti di lavoro includono clausole di riservatezza che rimangono valide anche dopo la cessazione del rapporto. La gestione di queste fasi è descritta nella "PRO Procedura di gestione delle risorse umane".

Gestione e Uso Accettabile degli Asset

Tutti gli asset informativi e le risorse associate devono essere identificati, classificati e protetti durante il loro ciclo di vita, come specificato nella **PRO Procedura di**

configurazione gestione e smaltimento degli asset e nella **POL Politica di classificazione ed etichettatura delle informazioni** . Il personale è tenuto a seguire le regole per l'uso accettabile delle risorse aziendali, che includono la politica della scrivania e dello schermo puliti per proteggere le informazioni sensibili da accessi non autorizzati. I beni utilizzati fuori sede devono essere protetti con misure adeguate, come descritto nella **POL Politica di sicurezza operativa** .

Gestione della Catena di Approvvigionamento

La sicurezza delle informazioni deve essere garantita lungo tutta la catena di approvvigionamento. Il **Responsabile Ufficio Acquisti (RACQ)** e il **Responsabile Qualifica Fornitori (RQF)** devono valutare i rischi di sicurezza associati a fornitori e partner, specialmente quelli che hanno accesso a informazioni aziendali, come dettagliato nella **PRO Procedura di gestione degli acquisti e delle terze parti** .

Sviluppo e Manutenzione dei Sistemi

La sicurezza è un requisito fondamentale in ogni fase del ciclo di vita dei sistemi informativi, dalla progettazione alla dismissione. I principi di "security by design" e "security by default" devono essere applicati, come definito nella **PRO Procedura di sviluppo sicuro** .

Gestione degli Incidenti di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni, osservato o sospetto, attraverso i canali designati. Il **Referente del Computer Security Incident Response Team (RCSIRT)** coordina la gestione degli incidenti secondo la **PRO Procedura di gestione degli incidenti di sicurezza delle informazioni** .

Continuità Operativa

Arakne deve garantire la capacità di continuare a operare durante e dopo eventi critici. Il **Direttore Tecnico (DIRTEC)** e il **Responsabile del Sistema Informativo (RSI)** sono responsabili della definizione e del test dei piani di continuità, come descritto nella **PRO Procedura di continuità operativa e di ripristino di emergenza** .

Conformità e Revisione

Il Sistema di Gestione della Sicurezza delle Informazioni è soggetto ad audit interni ed esterni per verificarne la conformità ai requisiti normativi (ISO/IEC 27001:2022, Direttiva NIS2), legali e contrattuali. La **Direzione Aziendale (DA)** riesamina periodicamente l'adeguatezza, l'idoneità e l'efficacia del SGSI. Questa politica viene riesaminata a intervalli pianificati e ogni qualvolta si verifichino cambiamenti significativi, come definito nella **PRO Procedura di gestione del cambiamento** , e viene comunicata a tutto il personale e alle parti interessate rilevanti.

Archiviazione e Aggiornamenti

La presente politica è gestita in formato controllato all'interno del sistema di gestione documentale aziendale. Viene riesaminata con cadenza almeno annuale, e ogni qualvolta si verifichino cambiamenti organizzativi, tecnologici o normativi significativi, per garantirne la continua idoneità, adeguatezza ed efficacia. Ogni aggiornamento è approvato dalla **Direzione Aziendale (DA)** .

Documenti di Riferimento

- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione dei rischi
- PRO Gestione riesame della direzione
- RA Ruoli Mansionario Responsabilita
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di configurazione gestione e smaltimento degli asset
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di sviluppo sicuro
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione del cambiamento