Ruoli e Responsabilità

Ruoli e responsabilità del Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

1. Scopo

Il presente documento definisce i ruoli funzionali e i relativi ambiti di responsabilità nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Forma Farm Srl.

L'obiettivo è assicurare che le responsabilità e le autorità rilevanti per la gestione della sicurezza delle informazioni siano chiaramente identificate, assegnate e comunicate, in coerenza con i requisiti della norma ISO/IEC 27001:2022.

Il modello organizzativo è proporzionato alle dimensioni e alla struttura di Forma Farm, che opera attraverso i propri soci e una rete di collaboratori e professionisti esterni, senza personale dipendente.

2. Principi organizzativi

L'organizzazione del SGSI si basa sui seguenti principi:

- **Attribuzione chiara delle responsabilità:** ogni funzione rilevante per la sicurezza delle informazioni deve avere responsabilità e autorità definite.

- **Flessibilità organizzativa:** uno stesso soggetto può ricoprire più ruoli funzionali, compatibilmente con le competenze necessarie e con l'eventuale presenza di conflitti di interesse.
- **Collaborazione tra soci e professionisti esterni:** le attività possono essere svolte da soci o collaboratori, nel rispetto degli incarichi, degli accordi contrattuali e delle autorizzazioni assegnate.
- **Separazione delle responsabilità:** ove necessario e proporzionato ai rischi, le funzioni di esecuzione, approvazione e verifica sono distinte. Quando la separazione non è concretamente possibile, sono previsti adeguati controlli compensativi.
- **Indipendenza delle verifiche:** le attività di audit interno sono organizzate in modo da garantire obiettività e imparzialità.

I ruoli descritti nel presente documento sono funzioni organizzative e non necessariamente posizioni lavorative o incarichi professionali autonomi.

3. Ruoli e responsabilità funzionali

La seguente tabella identifica i ruoli funzionali previsti nell'organizzazione del SGSI e ne descrive il rispettivo ambito di responsabilità.

Codice	Ruolo	Ambito di responsabilità
DIR	Direzione / Amministratore	Indirizzo e supervisione del SGSI; approvazione delle politiche e degli obiettivi di sicurezza; assegnazione delle risorse; approvazione delle decisioni di competenza in materia di gestione dei rischi; riesame delle prestazioni del SGSI.
RSI	Responsabile del SGSI	Coordinamento e mantenimento del SGSI; supporto all'analisi e al trattamento dei rischi; gestione della documentazione; monitoraggio degli obiettivi e delle azioni di miglioramento; coordinamento delle attività di verifica e reporting alla Direzione.
TEC	Responsabile tecnico e infrastrutture	Gestione della sicurezza delle infrastrutture e degli ambienti tecnologici; configurazioni e aggiornamenti; gestione tecnica degli accessi; backup e ripristino; monitoraggio; gestione delle vulnerabilità e degli interventi tecnici di sicurezza.

Codice	Ruolo	Ambito di responsabilità
SWD	Responsabile sviluppo software	Sicurezza del processo di sviluppo; gestione del codice sorgente e dei repository; controllo delle modifiche; gestione delle dipendenze software; verifiche e test; sicurezza dei rilasci e manutenzione applicativa.
PRI	Referente privacy e protezione dei dati	Coordinamento degli aspetti relativi alla protezione dei dati personali; supporto nella gestione degli adempimenti privacy, delle richieste degli interessati e delle violazioni di dati personali, in coordinamento con la Direzione e con le funzioni coinvolte.
COM	Responsabile commerciale e marketing	Gestione sicura delle informazioni commerciali; protezione dei dati di clienti e prospect; utilizzo sicuro degli strumenti CRM e marketing; riservatezza delle offerte e dei contratti; condivisione autorizzata delle informazioni con clienti e soggetti esterni.
HD	Responsabile helpdesk e assistenza clienti	Gestione e classificazione delle richieste di assistenza; supporto agli utenti; gestione dei ticket; accesso alle informazioni e ai sistemi dei clienti secondo le autorizzazioni ricevute; documentazione degli interventi e segnalazione di anomalie e incidenti.
VER	Verificatore / auditor interno	Pianificazione ed esecuzione delle verifiche interne sul SGSI; valutazione della conformità e dell'efficacia dei controlli; documentazione dei risultati degli audit e verifica delle azioni correttive, assicurando obiettività e imparzialità.

I ruoli possono essere ricoperti da più soggetti contemporaneamente. In particolare, le funzioni operative possono essere svolte da collaboratori esterni, mentre le responsabilità di coordinamento, supervisione e approvazione possono rimanere in capo ai soci o ad altri soggetti formalmente incaricati.

3.1 Collaboratori e fornitori esterni

Le attività affidate a collaboratori e fornitori esterni sono svolte nell'ambito degli incarichi e degli accordi contrattuali definiti con Forma Farm.

I collaboratori che partecipano alle attività del SGSI o che accedono a informazioni, sistemi e infrastrutture aziendali o dei clienti sono tenuti a:

- rispettare le politiche e le procedure di sicurezza applicabili;
- utilizzare esclusivamente gli accessi e le autorizzazioni assegnati;
- proteggere le informazioni e i dati trattati nello svolgimento delle attività;
- rispettare gli obblighi contrattuali di riservatezza e gli eventuali obblighi in materia di protezione dei dati personali;
- segnalare tempestivamente incidenti, anomalie o sospette violazioni della sicurezza.

La qualifica di socio o collaboratore non determina automaticamente l'attribuzione di specifiche responsabilità o autorizzazioni: queste sono definite in funzione dei ruoli effettivamente ricoperti e degli incarichi assegnati.

4. Assegnazione nominativa delle responsabilità

L'assegnazione dei ruoli funzionali ai singoli soggetti è documentata mediante una specifica matrice nominativa delle responsabilità RACI, riportata nel documento **«Matrice RACI – Assegnazione delle responsabilità SGSI»**.

La matrice associa le persone ai ruoli funzionali definiti nel presente documento, specificando per ciascun ruolo il livello di responsabilità attribuito:

- **A – Accountable:** responsabile ultimo del risultato e delle decisioni di propria competenza;
- **R – Responsible:** responsabile dell'esecuzione delle attività;
- **C – Consulted:** soggetto da consultare per competenze o contributi pertinenti;
- **I – Informed:** soggetto da informare sulle attività o decisioni rilevanti;
- **–:** nessuna responsabilità assegnata per il ruolo.

La matrice consente di rappresentare anche situazioni in cui uno stesso ruolo è ricoperto da più persone con livelli di responsabilità differenti, ad esempio quando un collaboratore svolge le attività operative e un socio mantiene la responsabilità ultima della funzione.

Per ciascun ruolo e per le responsabilità pertinenti deve essere identificato il soggetto dotato dell'autorità necessaria, evitando ambiguità nell'attribuzione delle decisioni.

5. Separazione dei compiti e controlli compensativi

Considerate le dimensioni dell'organizzazione e la possibilità che uno stesso soggetto ricopra più ruoli, Forma Farm valuta la separazione dei compiti in funzione della natura delle attività e dei rischi associati.

Particolare attenzione è riservata a:

- assegnazione e gestione delle autorizzazioni di accesso;
- attività tecniche con privilegi amministrativi;
- modifiche alle infrastrutture e agli ambienti di produzione;
- gestione degli incidenti di sicurezza;
- approvazione e verifica delle attività rilevanti;
- esecuzione degli audit interni.

Quando non è possibile realizzare una separazione diretta tra chi esegue e chi approva o verifica un'attività, possono essere adottati controlli compensativi, quali registrazione delle operazioni, revisione successiva, approvazione da parte della Direzione o verifica indipendente.

Le modalità di applicazione dei controlli sono definite nelle procedure operative pertinenti e documentate attraverso le relative evidenze.

6. Aggiornamento e riesame

Il presente documento e la relativa matrice RACI sono mantenuti aggiornati dal Responsabile del SGSI e sottoposti all'approvazione della Direzione.

Sono riesaminati in occasione di:

- variazioni nella composizione dei soci o dei collaboratori;
- assegnazione o cessazione di incarichi e responsabilità;
- modifiche significative all'organizzazione o ai servizi erogati;
- introduzione di nuove attività o sistemi che comportino responsabilità rilevanti per la sicurezza;
- riesame periodico del SGSI o rilevazione di criticità nell'attribuzione delle responsabilità.

Le modifiche alle assegnazioni nominative sono riportate nella matrice RACI, mentre il presente documento viene aggiornato quando cambiano i ruoli funzionali o i rispettivi ambiti di responsabilità.

7. Riferimenti

- ISO/IEC 27001:2022 – Clausola 5.3: Organizational roles, responsibilities and authorities.
- ISO/IEC 27001:2022 – Clausola 5.1: Leadership and commitment.
- ISO/IEC 27001:2022 – Clausola 7.2: Competence.
- ISO/IEC 27001:2022 – Clausola 7.3: Awareness.
- ISO/IEC 27001:2022 – Clausola 9.2: Internal audit.
- Matrice RACI – Assegnazione delle responsabilità SGSI.
- Politica per la sicurezza delle informazioni.
- Procedura di gestione degli accessi.
- Procedura di gestione degli incidenti di sicurezza.

Revision #2
Created 2026-10-22 09:17:05 UTC by Alberto Pastorelli
Updated 2026-10-30 20:05:22 UTC by Alberto Pastorelli