1. Verbale riesame della direzione

Verbale del Riesame della Direzione

Il presente verbale documentail riesame periodico della Direzione di DNS Informatica SAS, finalizzato a valutare l'efficacia e l'adeguatezza del Sistema di Gestione Integrato per la Qualità (ISO 9001:2015) e la Sicurezza delle Informazioni (ISO/IEC 27001:2022). Il riesame è condotto in conformità ai requisiti delle clausole 9.3 di entrambi gli standard, con l'obiettivo di garantire il miglioramentocontinuo, la conformità normativa e la protezione delle risorse informative aziendali.

1. Scopo e Campo di Applicazione

Il verbale riguarda la revisione delle prestazioni complessivedel Sistema di Gestione, includendol'analisi dei processi principali di DNS Informatica SAS, quali la gestione delle infrastrutture IT, la fornitura di servizi cloud, hosting, cybersecurity, VoIP e assistenza remota. Il riesame copre anche la valutazione delle azioni correttive, dei rischi residui e delle opportunità di miglioramento,in linea con il campodi applicazione certificato: "Erogazione di servizi informatici e di consulenza ICT, comprensivi di progettazione, implementazione,gestione e assistenza di infrastrutture informatiche, servizi cloud e soluzioni di cybersecurity".

2. Partecipanti e Responsabilità

La riunione è presieduta dal Referente della Direzione, Racca Marco, socio accomandatario, con la partecipazione dei responsabili dei processi chiave e del Responsabiledel Sistema di Gestione Integrato. La Direzione ha la responsabilità di assicurare che le decisioni prese siano coerenti con la politica aziendale,gli obiettivi strategici e i requisiti normativi applicabili, inclusi quelli relativi alla tutela della riservatezza, integrità e disponibilità delle informazioni (clausole 5.1 e 6.1 ISO 9001 e ISO/IEC 27001).

3. Input del Riesame

Il riesame si basa su dati oggettivi e documentati, quali:

• Risultati delle audit interne ed esterne (clausola 9.2 ISO 9001 e ISO/IEC 27001);

• Analisi delle non conformità e azioni correttive intraprese;

• Valutazione dei rischi e opportunità, inclusi quelli relativi alla sicurezza delle informazioni (clausola 6.1 ISO/IEC 27001);

• Feedback dei clienti e stakeholder;

• Prestazioni dei processi e conformità ai requisiti contrattuali;

• Aggiornamenti normativi e tecnologici rilevanti per il settore ICT e la cybersecurity;

• Risorse disponibili e necessità di formazione del personale (clausola 7.2 ISO 9001).

4. Analisi e Valutazione

Durante il riesame,la Direzione valuta l'efficacia delle misure di controllo implementateper mitigare i rischi identificati, con particolare attenzione alla protezione dei dati gestiti tramite sistemi informatici e procedure dedicate (clausola 8.1 ISO/IEC 27001). Si esaminanoinoltre le prestazioni operative dei processi di erogazione servizi, con indicatori chiave quali tempi di risposta, tassi di risoluzione delle anomalie e livelli di soddisfazione cliente.

L'analisi include la verifica della conformità alle disposizioni legislative e regolamentari applicabili, nonché la coerenza con la politica aziendale in materia di qualità e sicurezza delle informazioni. Eventuali scostamenti o criticità rilevate sono oggetto di discussione e pianificazione di azioni correttive o preventive.

5. Decisioni e Azioni

La Direzione definisce le azioni necessarie per migliorare l'efficacia del Sistema di Gestione, assegnando responsabilità e scadenze precise. Le decisioni possono riguardare:

• Aggiornamento delle procedure operative e delle misure di sicurezza;

• Investimenti in formazione specialistica per il personale;

• Implementazione di nuove tecnologie o strumenti per la gestione dei servizi cloud e della cybersecurity;

• Rafforzamento del monitoraggio dei fornitori e dei partner strategici;

• Revisione degli obiettivi di qualità e sicurezza per il periodo successivo.

6. Documentazione e Registrazioni

Il verbale del riesame è registrato come documento ufficiale del Sistema di Gestione Integrato e archiviato secondo le modalità previste dal piano di controllo documentale aziendale (clausola 7.5 ISO 9001). Le registrazioni includono:

• Elenco dei partecipanti e loro firme;

• Ordine del giorno e materiali di supporto;

• Risultati delle analisi e delle valutazioni;

• Azioni concordate con relativi responsabili e tempistiche;

• Indicatori di performance aggiornati.

Tali registrazioni costituiscono evidenza oggettiva per le attività di audit interno ed esterno e per la verifica della conformità ai requisiti ISO 9001 e ISO/IEC 27001.

7. Interfacce e Integrazione con Altri Processi

Il processo di riesame della Direzione interagisce strettamente con i processi di gestione del rischio, controllo delle forniture, gestione delle non conformità e miglioramento continuo. La Direzione assicura che le informazioni derivanti dal riesame siano comunicate efficacemente ai responsabili di processo e al personale coinvolto, favorendo un approccio integrato e sinergico tra qualità e sicurezza delle informazioni.

Placeholder diagramma di processo: Il diagramma illustrerà il flusso informativo e decisionale tra la Direzione, i responsabili di processo, il team di sicurezza ICT, e le funzioni operative coinvolte nel riesame e nell'attuazione delle azioni correttive e migliorative.

8. Monitoraggio e Verifica dell'Efficacia

La Direzione definisce indicatori specifici per monitorare l'efficacia delle azioni intraprese a seguito del riesame, quali:

• Riduzione delle non conformità ricorrenti;

• Miglioramento dei tempi di risposta e risoluzione;

• Incremento della soddisfazione cliente e stakeholder;

• Conformità continua ai requisiti di sicurezza delle informazioni.

Questi indicatori sono oggetto di verifica periodica e costituiscono elementi fondamentali per i successivi cicli di riesame e audit.

9. Conclusioni

Il verbale del riesame della Direzione rappresenta un documentochiave per la governance del Sistema di Gestione Integrato di DNS Informatica SAS, assicurando la coerenza tra strategia aziendale, requisiti normativi e aspettative dei clienti. La Direzione si impegnaa mantenereun approccio proattivo e basato su evidenzeper garantire la qualità dei servizi ICT e la sicurezza delle informazioni, in un contesto di continua evoluzione tecnologica e normativa.