TRANSTEC SERVICES S.R.L.

MANUALE SULLA SICUREZZA DELLE INFORMAZIONI

Rev.	Data	NOTA DI REVISIONE
1	23.07.2025	Revisione 1
0	22.04.2025	Prima emissione

Copia N.:	**Controllata SI ☐ NO ☐**	**Data consegna**	**Consegnata A**
Verificata RGI		Approvata AU	

INDICE

INTRODUZIONE

TransTec Services è una società di servizi e consulenza in grado di offrire specifiche conoscenze nell'ambito dell'ICT e dell'Innovazione Tecnologica, anche a livello internazionale.

Grazie all'elevata esperienza maturata nel settore, TransTec Services supporta i clienti nel processo di sviluppo tecnologico, offrendo prodotti innovativi e soluzioni mirate a rispondere a specifici obiettivi aziendali e a sviluppare nuovi modelli di business finalizzati all'eccellenza competitiva.

1 SCOPO E CAMPO DI APPLICAZIONE

TRANSTEC SERVICES S.R.L., consapevole dell'importanza strategica della protezione dei dati e della gestione sicura delle informazioni, ha adottato e implementato un Sistema di Gestione per la Sicurezza delle Informazioni conforme ai requisiti stabiliti dalla norma ISO/IEC 27001:2022.
Tale sistema è stato progettato con l'obiettivo di:

- Acquisire e mantenere un vantaggio competitivo, assicurando il rispetto rigoroso dei requisiti contrattuali stabiliti dai clienti, con un'attenzione prioritaria alla tutela della riservatezza, integrità e disponibilità delle informazioni a loro riferite.
- Effettuare in maniera obiettiva e strutturata l'identificazione, la valutazione e il trattamento dei rischi correlati alla sicurezza delle informazioni, promuovendo allo stesso tempo la formalizzazione e il miglioramento continuo di processi, procedure operative e documentazione associata.
- Assicurare il pieno rispetto delle normative vigenti, delle leggi nazionali e internazionali applicabili e dei regolamenti settoriali, fornendo evidenza tangibile della propria conformità attraverso verifiche, audit e controlli indipendenti.
- Dimostrare in modo trasparente e concreto l'impegno della Direzione e delle figure apicali aziendali nel garantire la protezione delle informazioni, integrando la sicurezza come parte integrante della cultura organizzativa e della governance.
- Monitorare costantemente le performance del sistema attraverso indicatori chiave e attività di controllo, attivando tempestivamente azioni correttive e di miglioramento in risposta a eventuali non conformità o nuove esigenze emergenti.

Il presente Manuale della Sicurezza delle Informazioni rappresenta il documento guida attraverso cui TRANSTEC SERVICES S.R.L. descrive l'approccio adottato per adempiere ai requisiti della norma ISO/IEC 27001:2022, nonché a quelli derivanti dalle leggi e regolamenti applicabili, con l'obiettivo di proteggere i beni informativi aziendali e assicurare un sistema di gestione efficiente, sostenibile e orientato al miglioramento continuo.

1.1 GENERALITÀ DELL'AZIENDA

Ragione sociale	TRANSTEC SERVICES S.R.L.
Sede legale	VIA CORNELIA 498 - ROMA (RM) – 00166
Sede operativa	VIA CORNELIA 498 - ROMA (RM) – 00166
C.F.- Partita I.V.A.	08393961001
Tel.	06 6390339

1.2 PRODOTTI E SERVIZI

L'ambito del campo di applicazione: "CONSULENZA DI NATURA INFORMATICA"

Servizi offerti dall'azienda:

TLC Consulting - TransTec Services, grazie alla comprovata esperienza maturata presso gli operatori italiani più importanti di Telecomunicazioni, è in grado di aiutare i propri Clienti a potenziare la loro competitività sia a livello tecnico che economico, incrementando l'efficienza dell'intero Network. I servizi di consulenza fanno riferimento alle attività di analisi, configurazione, progettazione, ottimizzazione e qualità della rete per tutte le tecnologie innovative in ambito TLC.

IT Consulting - TransTec Services si avvale di personale altamente specializzato e certificato e continuamente aggiornato sulle nuove tecnologie, per fornire consulenza sia nell'ambito della sicurezza informatica che nell'amministrazione di rete e sviluppo software, con l'obiettivo di offrire soluzioni personalizzate per soddisfare al meglio le esigenze del cliente.

1.3 APPROCCIO PER PROCESSI E RISK-BASED THINKING

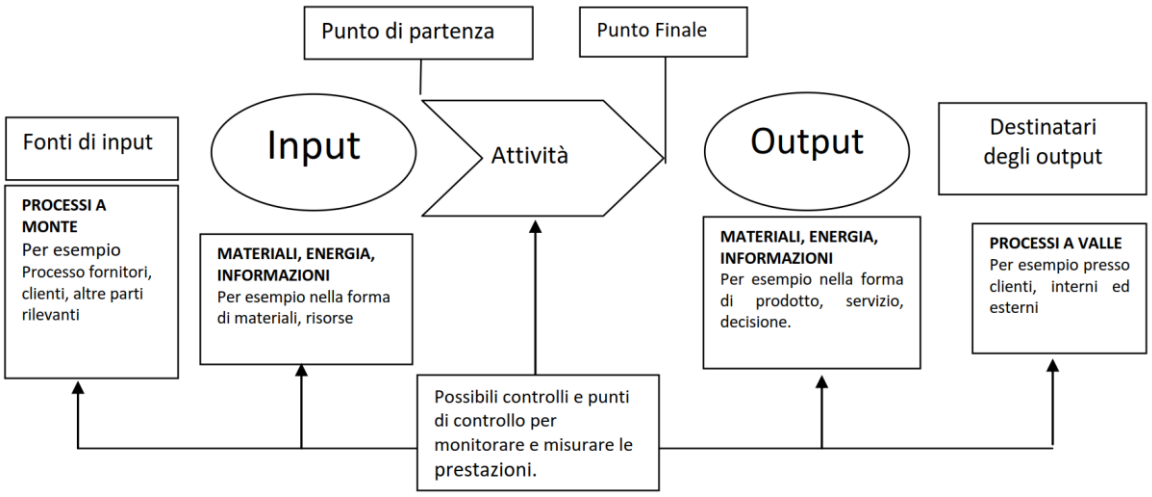
TRANSTEC SERVICES S.R.L. è fermamente convinta che il raggiungimento degli obiettivi aziendali – in termini di efficacia ed efficienza – sia possibile attraverso un approccio strutturato e sistematico alla gestione per processi.

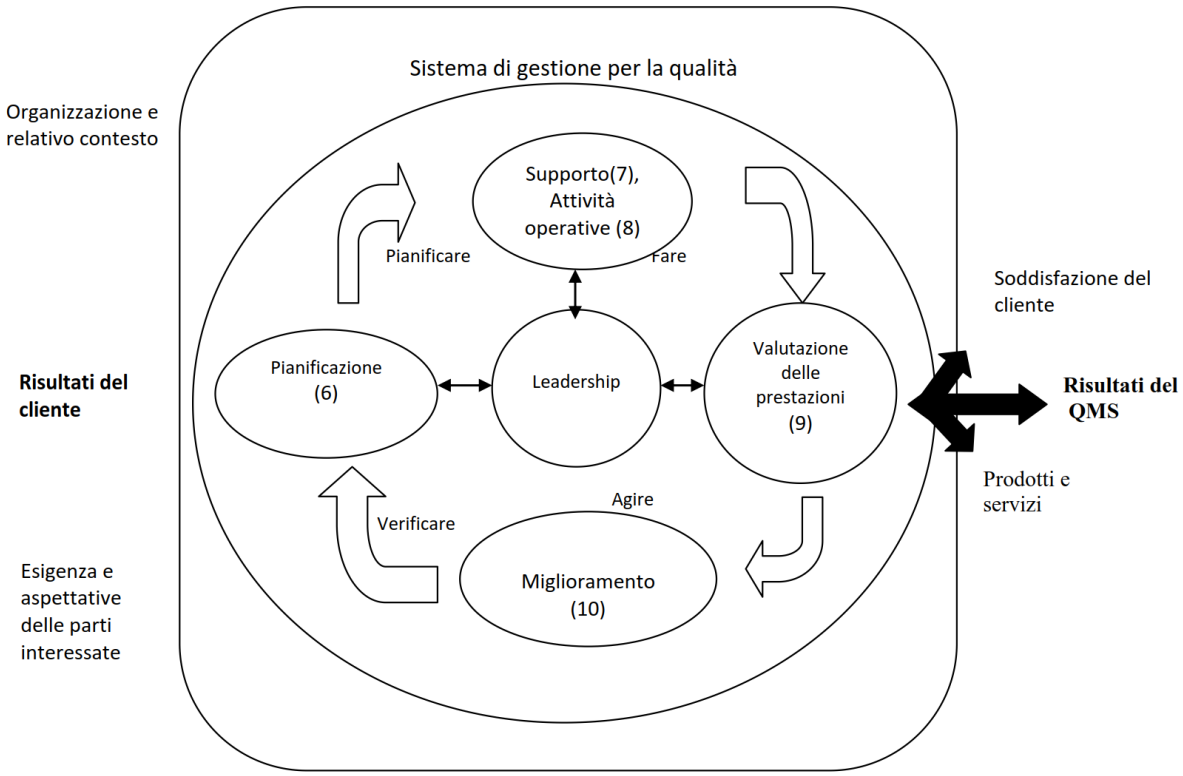
L'adozione di questo modello organizzativo consente di:

- Comprendere pienamente i requisiti dei clienti e delle parti interessate, assicurandone il soddisfacimento in modo costante e sostenibile nel tempo;
- Analizzare e gestire ciascun processo in funzione del valore aggiunto che è in grado di generare per l'organizzazione e per i suoi stakeholder;
- Perseguire con continuità il miglioramento delle performance, assicurando che ogni processo sia efficiente e orientato al raggiungimento dei risultati attesi;
- Promuovere un ciclo di miglioramento continuo, supportato dalla raccolta, valutazione e utilizzo sistematico di dati oggettivi e informazioni significative.

L'intero approccio si fonda sull'applicazione del ciclo di miglioramento continuo PLAN-DO-CHECK-ACT (PDCA), che guida l'organizzazione nella pianificazione, attuazione, verifica e miglioramento delle attività e dei processi.

Un elemento centrale di questo sistema è il Pensiero Basato sul Rischio, che permette di individuare preventivamente potenziali criticità, anticipare gli effetti indesiderati e definire azioni preventive efficaci, rafforzando così la capacità dell'azienda di gestire l'incertezza e cogliere le opportunità.





2 RIFERIMENTI NORMATIVI

L'azienda ha sviluppato il Sistema di Gestione per la Sicurezza delle Informazioni in conformità alle norme:

- UNI EN ISO 19011:2018 Linee guida per gli audit dei sistemi di gestione
- ISO/IEC 27000:2020 Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Panoramica e vocabolario
- ISO/IEC 27001:2022 Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni
- ISO/IEC 27002:2023 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni
- UNI EN ISO 31000:2018 Risk Management – Principi e linee guida

Sono considerate inoltre rilevanti ai fini della corretta implementazione del sistema le seguenti normative:

- Provvedimenti del Garante
- Reg. UE 679/2016 (GDPR)
- DECRETO LEGISLATIVO 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali

3 TERMINI E DEFINIZIONI

Azione correttiva: Azione per eliminare le cause di una non conformità rilevata, o di altre situazioni potenziali indesiderabili.

Certificazione di conformità: atto mediante il quale una terza parte indipendente dichiara che, con ragionevole attendibilità, un determinato

prodotto, processo o servizio e conforme ad una specifica norma o ad un altro documento normativo.

Conformità: soddisfacimento di un requisito

Controllo della Qualità: parte della gestione della qualità mirata a soddisfare i requisiti per la qualità.

Dichiarazione di conformità: dichiarazione di un fornitore, sotto la sua sola responsabilità, che un prodotto, processo o servizio è conforme ad una specifica norma o ad un altro documento normativo.

Gestione per la qualità: Attività coordinate per guidare e tenere sotto controllo un'azienda in materia di qualità.

Non Conformità: mancato soddisfacimento di un requisito.

Norma: documento, prodotto mediante consenso e approvato da un organismo riconosciuto, che fornisce, per usi comuni e ripetuti, regole, linee guida o caratteristiche, relative a determinate attività o ai loro risultati, al fine di ottenere il miglior ordine in un determinato contesto.

Parte interessata: persona o organizzazione che può avere influenza sull'organizzazione o che può essere influenzata da una decisione o da un'attività dell'organizzazione.

Politica per la qualità: Obiettivi ed indirizzi generali di un'Organizzazione, relativi alla qualità, espressi in modo formale dall'alta Direzione.

Qualità: grado in cui un insieme di caratteristiche intrinseche soddisfa i requisiti.

Rischio: grado di incertezza nel raggiungimento di un obiettivo.

Requisito: esigenza o aspettativa che può essere espressa, generalmente implicita o cogente.

Terzi, terza parte: persona o organismo riconosciuto come indipendente dalle parti coinvolte relativamente all'oggetto in questione.

Riservatezza: proprietà per la quale le informazioni non siano rese disponibili o divulgate ad individui non autorizzati

Executive management: persona o gruppo di persone ai quali è stata delegata la responsabilità dall'organo di governo per l'attuazione delle strategie e politiche atte a raggiungere l'obiettivo dell'organizzazione

Sicurezza delle informazioni: preservazione di riservatezza, integrità e disponibilità delle informazioni; in aggiunta, possono essere coinvolte anche altre proprietà quali autenticità, responsabilità, non misconoscimento e affidabilità

Continuità della sicurezza delle informazioni: processi/procedure atte a garantire continuità alla sicurezza delle informazioni

Incidente nella sicurezza delle informazioni: singolo o serie di eventi di sicurezza delle informazioni indesiderate o inattese che hanno una significativa probabilità di compromettere operazioni e minacciano la sicurezza delle informazioni

Integrità: la proprietà di salvaguardare l'accuratezza e la completezza

Valutazione del rischio: processo globale di analisi del rischio e stima del rischio.

Trattamento del rischio: processo di trattamento della scelta e dell'attuazione delle misure per modificare il rischio

Dichiarazione di applicabilità: dichiarazione documentata che descrive gli obiettivi del controllo e i controlli che sono pertinenti e applicabili al SGSI dell'organizzazione

Sistema IT: parte delle risorse infrastrutturali aziendali finalizzate al trattamento delle informazioni in formato elettronico. Si compone di un'architettura hardware (e del relativo software operativo e di supporto) e di un'architettura software (software applicativi e tools di sviluppo).

Piattaforma web: suite comprensiva di tecnologie web avanzate che supportano la vendita dei servizi e la gestione degli stessi, ideata per un uso autonomo.

Piattaforme servizi cloud: le piattaforme progettate ideate e realizzate, introducono un livello di astrazione delle risorse hardware del server,

permettendo la creazione di virtual machine i cui processi sono indipendenti fra loro.

Sistema Disaster Recovery: sistema per la progettazione e la realizzazione di strutture tecnologiche a supporto e garanzia in caso di eventi catastrofici che potrebbero inficiare sul business continuità aziendale.

Verifica: Conferma, sostenuta da evidenze oggettive, del soddisfacimento di requisiti specificati.

Asset: ciò che ha valore in un'organizzazione, sia esso un oggetto od un soggetto

Dati: le informazioni gestite all' interno dell'Azienda, siano esse informatiche e/o cartacee

Disponibilità: tutte le risorse hardware e software del sistema e i dati sono sempre accessibili a chi è autorizzato, escludendo i casi di guasti

Confidenzialità: le informazioni sono accessibili in lettura solo a chi è autorizzato, protette contro letture accidentali o dolose di terze parti non autorizzate

Integrità: i dati informatici sono identici ai dati dei documenti originali da cui sono stati estratti, e non sono esposti ad accidentali o maliziose alterazioni o distruzioni

Sicurezza dell'informazione: preservazione della confidenzialità, integrità e disponibilità dell'informazione; in aggiunta, altri fattori come l'autenticità, la responsabilità, il non ripudio e l'affidabilità

Evento: un evento identificato di un sistema, servizio o condizione riguardante una possibile violazione della policy di sicurezza o fallimento delle disposizioni adottate o una situazione sconosciuta in precedenza che può divenire rilevante ai fini della sicurezza

Incidente: un singolo o una serie di non voluti od imprevisti eventi che possono avere una probabilità di compromettere le operazioni di business e di minacciare la sicurezza dell'informazione

Rischio residuo: ciò che rimane a seguito del trattamento del rischio

Accettazione del rischio: decisione di accettare il rischio

Risk analysis: uso di informazioni per identificare le fonti e valutare il rischio

Risk assessment: processo di risk analysis e della sua valutazione

Valutazione del rischio: processo di comparazione del rischio stimato con il criterio dato per determinare l'importanza del rischio

Risk management: coordinamento di attività atte a dirigere e controllare un'organizzazione ai fini del rischio

Trattamento del rischio: processo di selezione e implementazione di misure per modificare il rischio

Statement of applicability: documento che descrive gli oggetti e le misure di controllo applicabili all'intera organizzazione o ad una sua parte.

Data Breach: violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico;

Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Titolare dei dati personali: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Interessato: la persona fisica, cui si riferiscono i dati personali;

Responsabile dei dati personali: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Trattamento di dati personali: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il

raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

3.1 ABBREVIAZIONI

MSI Manuale per la Sicurezza delle Informazioni

SGSI Sistema di Gestione per la Sicurezza delle Informazioni

AC Azione Correttiva

ODC Organismo di certificazione

NC Non conformità

4 CONTESTO DELL'ORGANIZZAZIONE

L'Azienda ha identificato come elemento fondamentale per l'efficacia del proprio Sistema di Gestione per la Sicurezza delle Informazioni l'analisi costante del contesto in cui opera. In tale ottica, essa determina, verifica e riesamina periodicamente i fattori interni ed esterni che possono influenzare la propria capacità di:

- Fornire in modo continuativo prodotti e/o servizi conformi ai requisiti stabiliti dai clienti;
- Rispettare tutte le disposizioni legislative e regolamentari applicabili;
- Conseguire gli obiettivi prefissati all'interno del sistema di gestione della sicurezza delle informazioni.

L'analisi del contesto tiene conto di variabili esterne, come l'evoluzione normativa, le tendenze di mercato, i cambiamenti tecnologici e le aspettative delle parti interessate, nonché di fattori interni, quali la struttura organizzativa, le risorse disponibili, la cultura aziendale e i processi operativi.

Questa valutazione viene effettuata in modo strutturato e documentato, al fine di garantire che il sistema di gestione rimanga adeguato, pertinente ed efficace, anche in presenza di cambiamenti significativi. L'approccio adottato consente inoltre di anticipare eventuali rischi, cogliere opportunità di miglioramento e allineare le strategie aziendali alla missione dell'organizzazione e alla protezione dei propri asset informativi.

4.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO

TRANSTEC SERVICES S.R.L., nell'ambito dell'implementazione e del mantenimento del proprio Sistema di Gestione per la Sicurezza delle Informazioni, ha identificato e analizzato in maniera sistematica le questioni interne ed esterne che risultano rilevanti per le attività aziendali e per la definizione della propria pianificazione strategica.
Tali questioni sono valutate in funzione della loro potenziale influenza sulla capacità dell'organizzazione di raggiungere gli obiettivi stabiliti in materia di

sicurezza delle informazioni, garantendo al contempo la conformità ai requisiti normativi, contrattuali e alle aspettative delle parti interessate.

Nel contesto esterno, sono considerate tutte le variabili – a livello internazionale, nazionale, regionale e locale – che possono impattare, direttamente o indirettamente, sulla sicurezza delle informazioni. In particolare, rientrano tra queste:

- l'ambiente legale e normativo, inteso come l'insieme di leggi, regolamenti e obblighi cogenti;
- il contesto tecnologico, comprensivo delle innovazioni e dei cambiamenti nei sistemi informatici e nelle infrastrutture digitali;
- l'ambiente competitivo, ovvero la presenza e le strategie dei concorrenti sul mercato;
- il mercato di riferimento, con le sue dinamiche, esigenze e tendenze evolutive;
- il contesto culturale, sociale ed economico, che influenza i comportamenti delle parti interessate e l'adozione di pratiche di sicurezza;
- il quadro giuridico, con riferimento sia alle normative generali che a quelle settoriali.

All'interno dell'organizzazione, sono oggetto di analisi e monitoraggio i fattori che riflettono la sua struttura, identità e funzionamento. Tra questi si evidenziano:

- i valori aziendali, che guidano le scelte strategiche e operative;
- la cultura organizzativa e il patrimonio di conoscenze e competenze interne;
- le prestazioni dei processi e dei sistemi aziendali, misurate attraverso indicatori e obiettivi;
- l'assetto organizzativo, ovvero ruoli, responsabilità e modalità di coordinamento;
- le caratteristiche dell'ambiente fisico, incluse le infrastrutture e i luoghi di lavoro.
- gli aspetti logici, relativi alla gestione e protezione degli asset informatici, delle reti, dei sistemi e dei dati digitali.

L'analisi del contesto viene riesaminata con regolarità e ogniqualvolta si verifichino cambiamenti significativi, al fine di assicurare che il sistema di gestione sia sempre coerente con le esigenze operative e aggiornato rispetto al contesto dinamico in cui opera l'azienda.

4.2 COMPRENDERE I BISOGNI E LE ASPETTATIVE DELLE PARTI INTERESSATE

TRANSTEC SERVICES S.R.L., nell'ambito della gestione efficace del proprio Sistema di Gestione per la Sicurezza delle Informazioni, ha effettuato un'attenta identificazione delle parti interessate (stakeholders) che possono influenzare – anche in modo potenziale – la capacità dell'organizzazione di erogare prodotti e servizi conformi ai requisiti contrattuali dei clienti, nonché agli obblighi legali e regolamentari applicabili.
Per ciascuna parte interessata individuata, l'azienda ha determinato i requisiti rilevanti, siano essi espliciti (espressi in contratti, leggi o normative) o impliciti (derivanti da aspettative legittime, prassi consolidate o responsabilità etiche).
L'obiettivo è garantire che tali requisiti siano presi in considerazione nella pianificazione, nello sviluppo e nel miglioramento continuo del sistema di gestione.
Le principali parti interessate identificate includono:

- La Proprietà: responsabile dell'indirizzo strategico e del supporto decisionale, interessata alla protezione degli asset aziendali, alla reputazione e alla sostenibilità dell'impresa.
- I Clienti diretti: destinatari dei prodotti e servizi offerti, portatori di requisiti specifici in termini di qualità, sicurezza delle informazioni, tempi di consegna e conformità normativa.
- I Fornitori e i Partner: soggetti esterni che contribuiscono, direttamente o indirettamente, all'erogazione dei servizi; la loro affidabilità e conformità ai requisiti di sicurezza è cruciale per la catena del valore.
- Gli Enti Regolatori e la Pubblica Amministrazione: istituzioni che emettono e fanno rispettare normative cogenti, requisiti settoriali e standard di sicurezza applicabili al contesto operativo dell'organizzazione.
- Il Settore del Credito: banche, istituti finanziari e assicurativi che interagiscono con l'organizzazione e ne influenzano le condizioni operative, in particolare in ambito di conformità, trasparenza e gestione del rischio.

- L'Ambiente: inteso sia in senso fisico (con attenzione all'impatto ambientale delle attività aziendali) sia come contesto socio-economico in cui l'impresa opera, che può influenzare la percezione della responsabilità sociale e della sostenibilità.
- I Lavoratori e i Collaboratori: risorse interne ed esterne il cui coinvolgimento, formazione e consapevolezza sono essenziali per l'efficacia del SGSI e per la protezione delle informazioni trattate.

TRANSTEC SERVICES S.R.L. monitora costantemente le esigenze e le aspettative delle parti interessate, aggiornando tale analisi in caso di cambiamenti significativi in sede di Riesame della Direzione, per garantire che il sistema di gestione rimanga pertinente, efficace e allineato al contesto in evoluzione.

4.3 SCOPO DEL SISTEMA DI GESTIONE SULLA SICUREZZA DELLE INFORMAZIONI

Attraverso lo sviluppo e l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001:2022, TRANSTEC SERVICES S.R.L. si pone l'obiettivo di garantire un approccio strutturato, sistematico e sostenibile alla gestione della sicurezza delle informazioni, in linea con le proprie strategie aziendali e le aspettative delle parti interessate.

L'adozione del SGSI consente all'organizzazione di:

- Monitorare e tenere sotto controllo il contesto organizzativo interno ed esterno, valutandone in modo continuo gli impatti sulla sicurezza delle informazioni e sull'efficacia del sistema di gestione;

- Mantenere e incrementare la soddisfazione del cliente, assicurando che i servizi e le soluzioni fornite siano conformi ai requisiti di sicurezza, riservatezza, integrità e disponibilità delle informazioni trattate;

- Identificare, analizzare e gestire in modo proattivo i rischi e le opportunità, promuovendo un approccio basato sulla prevenzione e sull'adattabilità ai cambiamenti;

- Salvaguardare e rafforzare la solidità patrimoniale dell'organizzazione, sostenendo la continuità operativa e contribuendo alla redditività nel lungo periodo attraverso una gestione consapevole della sicurezza delle informazioni;

- Soddisfare le aspettative della proprietà, in termini di ritorno sull'investimento, stabilità degli assetti organizzativi e capacità dell'impresa di operare in un contesto sicuro e controllato.

Il SGSI descritto nel presente Manuale è applicato in conformità alla norma UNI CEI EN ISO/IEC 27001:2022, e copre nello specifico il seguente ambito operativo:

INSTALLAZIONE, CONSULENZA E COMMERCIALIZZAZIONE DI SISTEMI HARDWARE E SOFTWARE

Tale ambito comprende tutte le attività, i processi e le risorse coinvolte nella gestione e nello sviluppo di soluzioni digitali e sistemi critici, con l'obiettivo di assicurare che la protezione delle informazioni sia parte integrante della qualità e dell'affidabilità dei servizi offerti da TRANSTEC SERVICES S.R.L.

4.4 SISTEMA DI GESTIONE SULLA SICUREZZA DELLE INFORMAZIONI E RELATIVI PROCESSI

La documentazione del Sistema è strutturata nel seguente modo:

MANUALE

Il Manuale per la Sicurezza delle Informazioni rappresenta il documento di riferimento che formalizza e comunica la Politica della Direzione in materia di protezione delle informazioni e gestione dei rischi ad esse associati.

Attraverso il manuale, l'organizzazione:

- Definisce l'approccio adottato per garantire la sicurezza delle informazioni in tutte le attività rilevanti, in linea con gli obiettivi aziendali, i requisiti normativi e le aspettative delle parti interessate;
- Stabilisce le disposizioni generali e i principi organizzativi che regolano i processi aziendali aventi impatto diretto o indiretto sulla sicurezza delle informazioni;
- Descrive il campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), specificando in modo trasparente eventuali esclusioni debitamente giustificate e documentate;
- Fornisce una visione integrata e coerente del modello organizzativo adottato, promuovendo una gestione sistematica della sicurezza e una cultura della prevenzione.

Alcuni capitoli del Manuale includono o fanno esplicito riferimento alle Procedure per la Sicurezza delle Informazioni che disciplinano in dettaglio le attività operative, i controlli e le responsabilità associate.
L'elenco completo e aggiornato di tali procedure è riportato in un apposito capitolo del Manuale, così da garantire chiarezza, tracciabilità e facile accesso alla documentazione operativa prevista dal SGSI.

La gestione, diffusione e aggiornamento del Manuale per la Sicurezza delle Informazioni è regolata da precise modalità operative al fine di garantire il controllo documentale e la tracciabilità delle versioni in uso.

Il Responsabile per la Sicurezza delle Informazioni (RSI) conserva tutte le copie non distribuite del Manuale, assicurandone l'integrità e il controllo.

In fase di distribuzione, il RSI:

- Attribuisce un'identificazione univoca a ciascuna copia rilasciata;
- Verifica la completezza del contenuto e la conformità all'ultima versione approvata;
- Compila la pagina identificativa della copia, riportando le informazioni essenziali per il tracciamento e apponendo la propria sigla quale attestazione di validità.

L'indice generale del Manuale è sottoposto ad approvazione formale da parte della Direzione, come evidenza di validazione ufficiale.

Le copie ufficiali del Manuale vengono distribuite internamente secondo la seguente assegnazione:

- n° 1 copia alla Direzione

- n°1 copia all'Ufficio del Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RGSI)

Tutte le copie distribuite sono sotto il controllo diretto del RGSI, il quale è incaricato di:

- Provvedere all'aggiornamento simultaneo di tutte le copie in caso di modifiche o revisioni;
- Mantenere un registro di distribuzione aggiornato;
- Garantire che le copie obsolete vengano ritirate o chiaramente identificate come non valide.

L'eventuale rilascio del Manuale o di sue parti a soggetti esterni è consentito solo previa autorizzazione formale del Responsabile per la Sicurezza delle Informazioni, che valuta la legittimità e la necessità della diffusione.

Tutte le copie interne sono soggette a processo di revisione, assicurato dal RSI. Ogni modifica apportata al Manuale viene evidenziata in appositi paragrafi dedicati alle revisioni, così da garantire trasparenza, tracciabilità delle modifiche e corretta applicazione delle versioni aggiornate.

PROCEDURE

Le Procedure per la Sicurezza delle Informazioni costituiscono parte integrante del Sistema di Gestione per la Sicurezza delle Informazioni e rappresentano gli strumenti operativi attraverso cui l'organizzazione attua, controlla e mantiene efficace il sistema stesso.
Tali procedure:

- Descrivono in modo dettagliato i processi, le attività e i controlli necessari per implementare correttamente il SGSI in conformità ai requisiti della norma ISO/IEC 27001, assicurando che tutte le funzioni aziendali coinvolte operino in modo coerente con gli obiettivi di sicurezza delle informazioni;
- Definiscono le sequenze logiche, le responsabilità e le interazioni tra i processi, con l'obiettivo di garantire che le informazioni trattate siano gestite nel rispetto dei requisiti di riservatezza, integrità e disponibilità, nonché della conformità normativa, contrattuale e interna;
- Sono strutturate per favorire l'applicazione sistematica dei controlli di sicurezza, promuovendo un approccio documentato e ripetibile alla gestione dei rischi informativi.

Le Procedure sulla Sicurezza delle Informazioni sono distribuite a tutto il personale coinvolto nei processi rilevanti, affinché ciascuno possa operare con piena consapevolezza del proprio ruolo e delle misure di sicurezza da applicare. La loro conoscenza e applicazione è obbligatoria per tutti coloro che partecipano, direttamente o indirettamente, all'attuazione del SGSI.

Ogni procedura può includere, come parte integrante, allegati, moduli e schede operative necessari alla registrazione, al monitoraggio e alla tenuta sotto controllo delle attività previste. Tali documenti supportano la tracciabilità delle azioni svolte, facilitano l'evidenza della conformità e contribuiscono al miglioramento continuo del sistema.

Le procedure sono soggette a controllo documentale, aggiornamento periodico e approvazione formale, in modo da assicurare che siano sempre attuali, adeguate ed efficaci rispetto al contesto organizzativo e agli obiettivi del SGSI.

MODULISTICA OPERATIVA

Altri documenti che contengono, o in cui vengono registrate, informazioni documentate, e che sono richiamati sia nel Manuale per la Sicurezza delle Informazioni che nelle Procedure sulla Sicurezza delle Informazioni, comprendono una varietà di strumenti progettati per supportare e garantire l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI). Questi documenti sono essenziali per l'implementazione pratica delle politiche e delle procedure aziendali, e sono utilizzati per descrivere in dettaglio le modalità operative necessarie per il controllo e la gestione della sicurezza delle informazioni all'interno dell'organizzazione.
I principali strumenti documentali includono:

- Piani: che definiscono gli obiettivi, le attività e le risorse necessarie per il raggiungimento degli scopi stabiliti nell'ambito della sicurezza delle informazioni.
- Moduli e schede: che vengono utilizzati per registrare informazioni in modo strutturato e sistematico.
- Check list: che offrono una lista predefinita di elementi da verificare o attività da completare.

5 LEADERSHIP

5.1 LEADERSHIP E IMPEGNO

La Direzione conferma il proprio pieno impegno nello sviluppo, nell'attuazione, nella gestione e nel continuo miglioramento dell'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), in conformità ai requisiti della norma ISO/IEC 27001. Tale impegno si concretizza attraverso una serie di azioni strategiche e operative, finalizzate a garantire che la sicurezza delle informazioni sia integrata nei processi organizzativi e sostenuta in modo sistemico. In particolare, la Direzione si impegna a:

- Comunicare costantemente e in modo chiaro a tutti i livelli dell'organizzazione l'importanza di rispettare sia i requisiti espressi dai clienti, sia quelli normativi, legali e regolamentari applicabili, al fine di assicurare la conformità e la fiducia degli stakeholder;
- Definire, formalizzare e diffondere la politica per la sicurezza delle informazioni, assicurandosi che essa sia adeguata allo scopo dell'organizzazione, supporti la direzione strategica aziendale e costituisca un riferimento per la definizione degli obiettivi specifici di sicurezza;
- Stabilire obiettivi misurabili per la sicurezza delle informazioni, assicurando che siano coerenti con la politica definita e che rispecchino l'evoluzione del contesto interno ed esterno dell'organizzazione, nonché i rischi identificati;
- Effettuare periodici riesami della Direzione (Management Review), al fine di valutare l'adeguatezza, l'efficacia e il miglioramento continuo del SGSI, anche in funzione di cambiamenti organizzativi, tecnologici o normativi;
- Garantire la disponibilità delle risorse necessarie, siano esse umane, tecnologiche o finanziarie, affinché il SGSI possa essere efficacemente implementato, mantenuto e migliorato;
- Promuovere una cultura organizzativa basata sulla consapevolezza, sulla responsabilità individuale e sull'adozione di un approccio orientato ai processi e al miglioramento continuo, al fine di rafforzare la resilienza e la protezione delle informazioni;
- Coinvolgere attivamente, motivare e guidare il personale a tutti i livelli, affinché comprenda il proprio ruolo e contribuisca concretamente al

raggiungimento degli obiettivi del SGSI, favorendo un clima collaborativo e orientato ai risultati;
- Supportare e responsabilizzare i ruoli di leadership presenti all'interno dell'organizzazione, affinché ciascuno, nell'ambito delle proprie competenze e responsabilità, dimostri un comportamento coerente con i principi della sicurezza delle informazioni, fungendo da esempio per il resto del personale.

5.2 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Gli obiettivi principali della Politica per la Sicurezza delle Informazioni sono:
- Soddisfare i requisiti, le esigenze e le aspettative dei clienti e delle parti interessate, garantendo la protezione delle informazioni trattate, anche attraverso livelli di servizio che siano coerenti con gli accordi contrattuali e competitivi sul mercato;
- Assicurare la conformità ai requisiti legali, normativi e contrattuali applicabili in materia di sicurezza delle informazioni, sia a livello nazionale che internazionale;
- Prevenire e minimizzare il rischio di violazioni, errori, incidenti o perdite di dati, attraverso l'adozione di controlli tecnici, organizzativi e procedurali appropriati, formalizzati all'interno del SGSI;
- Garantire che tutto il personale coinvolto nelle attività aziendali sia adeguatamente formato, consapevole delle proprie responsabilità e qualificato per contribuire attivamente alla protezione delle informazioni e al miglioramento continuo del sistema;
- Valutare e qualificare in modo rigoroso fornitori e partner esterni, affinché rispettino standard di sicurezza delle informazioni compatibili con quelli adottati internamente, promuovendo la sicurezza lungo tutta la catena di fornitura;
- Gestire e registrare sistematicamente gli eventi di sicurezza e le non conformità, identificandone le cause, adottando misure correttive efficaci e prevenendo il loro ripetersi, in linea con procedure documentate;
- Utilizzare attivamente i dati provenienti da audit interni, incidenti, segnalazioni e feedback del mercato, per guidare il miglioramento continuo del SGSI e delle misure di sicurezza implementate;
- Stabilire obiettivi specifici e misurabili per la sicurezza delle informazioni, periodicamente rivisti e aggiornati per garantire la loro coerenza con il

contesto aziendale, l'evoluzione dei rischi e la strategia dell'organizzazione.

La Direzione, con il supporto del Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni, ha il compito di assicurare che:

- La politica venga formalmente documentata, comunicata, compresa e sostenuta a tutti i livelli dell'organizzazione tramite distribuzioni di documentazione, riunioni o sedute formative ed affissione in bacheca;
- Le risorse umane, tecniche ed economiche necessarie siano rese disponibili per l'attuazione del SGSI;
- Tutti i dipendenti comprendano il proprio ruolo nel garantire la sicurezza delle informazioni;
- Venga promossa una cultura della sicurezza basata sulla responsabilità condivisa e sul miglioramento continuo;
- Vengano condotti audit interni e riesami della direzione almeno annuali per verificare l'adeguatezza, la validità e l'efficacia del SGSI, nonché la necessità di modificare o aggiornare la politica stessa.

5.3 RUOLI, RESPONSABILITÀ E AUTORITÀ

La Direzione garantisce che responsabilità, autorità e competenze siano chiaramente definite, documentate, comunicate e comprese all'interno dell'organizzazione, in conformità ai requisiti della norma ISO/IEC 27001:2022. Tali elementi sono formalizzati attraverso l'organigramma aziendale e il mansionario, i quali costituiscono strumenti fondamentali per la corretta gestione delle risorse e per il governo del SGSI.

In particolare, il mansionario include:

- La definizione puntuale delle competenze, delle responsabilità e delle autorità assegnate ai ruoli coinvolti nella gestione e protezione delle informazioni, con particolare attenzione ai processi critici e alle aree sensibili;
- I requisiti minimi per ciascun ruolo, inclusi titolo di studio, formazione specifica, abilità personali, esperienze pregresse e caratteristiche attitudinali, al fine di garantire l'idoneità delle risorse alle attività assegnate.

L'organigramma aziendale aggiornato e nominativo è reso disponibile a tutto il personale, assicurando trasparenza nella comunicazione delle responsabilità e delle linee di riporto funzionali.

L'adozione e la diffusione di tali strumenti ha l'obiettivo di:

- Assicurare che il Sistema di Gestione per la Sicurezza delle Informazioni sia implementato, mantenuto e migliorato in piena conformità ai requisiti della ISO/IEC 27001:2022;
- Garantire che i processi aziendali interagiscano in modo efficace, generando gli output attesi e contribuendo al raggiungimento degli obiettivi di sicurezza;
- Assicurare che vengano riferite alla Direzione le prestazioni del SGSI, le eventuali non conformità, le opportunità di miglioramento, nonché le necessità di cambiamento o innovazione;
- Promuovere, in tutta l'organizzazione, la consapevolezza in merito ai requisiti di sicurezza delle informazioni, inclusi quelli contrattuali, normativi e regolamentari;
- Garantire che l'integrità del SGSI sia mantenuta anche durante eventuali cambiamenti, pianificati o emergenti, relativi alla struttura, ai processi o alle tecnologie dell'organizzazione.

A supporto di queste attività e in coerenza con quanto previsto dalla norma, la Direzione ha formalmente designato, mediante apposita lettera di nomina, un Responsabile per la Sicurezza delle Informazioni (RSGSI).

Il RSGSI, indipendentemente da eventuali altre responsabilità operative o gestionali, ha il compito di:

- Supportare la Direzione nella pianificazione, attuazione, monitoraggio e miglioramento del SGSI;
- Coordinare le attività inerenti la gestione dei rischi per la sicurezza delle informazioni;
- Promuovere la conformità normativa e la cultura della sicurezza all'interno dell'organizzazione;
- Verificare l'efficacia delle azioni correttive e preventive;
- Collaborare alla gestione degli incidenti e alla revisione dei controlli, in linea con le esigenze dell'organizzazione e l'evoluzione del contesto esterno.

6 PIANIFICAZIONE

6.1 AFFRONTARE RISCHI ED OPPORTUNITÀ

In linea con i requisiti della norma ISO/IEC 27001:2022, la pianificazione delle attività e dei processi aziendali è strutturata in modo da garantire il controllo preventivo, la tracciabilità e la conformità delle operazioni, nonché la protezione contro i rischi potenziali legati alla sicurezza delle informazioni.
La pianificazione è formalizzata attraverso procedure operative e istruzioni documentate, che:

- Definiscono in modo chiaro le responsabilità associate a ciascuna attività;
- Specificano la sequenza logica delle operazioni da eseguire per il corretto svolgimento dei processi;
- Includono, ove necessario, l'elaborazione di Piani Specifici (es. piani di trattamento del rischio, piani di risposta a incidenti) qualora le sole procedure generali non risultino sufficienti a garantire il raggiungimento dei requisiti di sicurezza o l'efficace mitigazione dei rischi.

Tutte le attività e i processi, inclusa la redazione e il mantenimento del presente Manuale del SGSI, sono progettati e condotti secondo il modello ciclico PDCA (Plan – Do – Check – Act). Questo approccio consente:

- Una pianificazione proattiva basata sulla valutazione dei rischi e delle opportunità;
- Un controllo continuo durante l'esecuzione delle attività;
- Una gestione efficace dei feedback e delle non conformità, con l'obiettivo di alimentare un ciclo di miglioramento continuo.

La valutazione e il trattamento dei rischi per la sicurezza delle informazioni sono regolamentati attraverso specifiche procedure di analisi e gestione del rischio e documentati in apposito modulo, allegato al SGSI. Questi strumenti consentono di mantenere una visione aggiornata e dinamica del contesto di rischio, assicurando una risposta coerente e tempestiva.
Al fine di perseguire gli obiettivi di sicurezza delle informazioni, TRANSTEC SERVICES S.R.L. stabilisce periodicamente obiettivi misurabili e coerenti con la politica del SGSI.
Tali obiettivi:

- Sono formulati in termini quantificabili, oggettivi e verificabili;
- Possono essere articolati in obiettivi intermedi nei casi in cui il raggiungimento dell'obiettivo principale richieda un approccio graduale;
- Sono soggetti a monitoraggio e verifica da parte del Responsabile per la Sicurezza delle Informazioni (RSGSI);

- Sono oggetto di valutazione periodica in sede di Riesame della Direzione per valutarne il grado di raggiungimento e adottare eventuali azioni correttive o di miglioramento.

L'organizzazione, inoltre, dettaglia le risorse necessarie per ciascun obiettivo, incluse le responsabilità assegnate, i tempi previsti di attuazione e i criteri di verifica. Questo assicura un monitoraggio strutturato e tracciabile dei progressi compiuti.

La Direzione si impegna a rendere disponibili tutte le risorse necessarie per l'attuazione, la gestione e il miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni. Tali risorse comprendono:

- Risorse tecniche, infrastrutturali e informatiche;
- Competenze professionali e formazione continua del personale;
- Risorse per le attività di verifica e controllo, incluse le verifiche ispettive interne.

Le necessità e l'adeguatezza delle risorse vengono riesaminate periodicamente durante il Riesame della Direzione, al fine di assicurare la piena efficacia del SGSI anche in caso di cambiamenti organizzativi, tecnologici o normativi.

6.2 OBIETTIVI SULLA SICUREZZA DELLE INFORMAZIONI

La Direzione di TRANSTEC SERVICES S.R.L. stabilisce, comunica e riesamina regolarmente obiettivi specifici per la sicurezza delle informazioni. Tali obiettivi sono definiti con riferimento ai diversi livelli, funzioni e processi aziendali, e vengono gestiti formalmente attraverso apposito Piano di Miglioramento per la Sicurezza delle Informazioni.

Gli obiettivi sono comunicati internamente mediante canali strutturati di comunicazione interfunzionale, per garantire che le funzioni responsabili siano consapevoli del proprio contributo e delle azioni richieste per il loro raggiungimento. La Direzione, mediante riesami periodici, in particolare durante il Riesame della Direzione, verifica che tali obiettivi siano:

- Coerenti con la politica per la sicurezza delle informazioni e aggiornati in base all'evoluzione del contesto organizzativo o normativo;
- Pertinenti alla conformità dei prodotti e dei servizi, in relazione ai requisiti interni, contrattuali, normativi e cogenti applicabili;
- Orientati alla riduzione dei rischi, al miglioramento continuo e alla salvaguardia della riservatezza, integrità e disponibilità delle informazioni.

In fase di pianificazione degli obiettivi, TRANSTEC SERVICES S.R.L. determina per ciascuno di essi:

- Le azioni operative necessarie per il loro conseguimento;
- Le risorse richieste (in termini di personale, strumenti, infrastrutture e investimenti);
- Il responsabile designato al raggiungimento dell'obiettivo;
- I tempi di attuazione e le relative scadenze intermedie, ove applicabili;
- I criteri, metodi e frequenze di misurazione per valutare l'efficacia delle azioni intraprese e il livello di raggiungimento degli obiettivi.

Tutti gli obiettivi sono definiti secondo criteri di misurabilità, oggettività e coerenza con la politica aziendale. I dati vengono raccolti e analizzati attraverso indicatori di performance, che consentono un controllo continuo delle attività e l'adozione tempestiva di azioni correttive o preventive.

Il Piano di Miglioramento della Sicurezza delle Informazioni include per ciascun obiettivo:

- L'identificazione del processo aziendale coinvolto;
- La definizione specifica dell'obiettivo correlato;
- Il valore di riferimento dell'indicatore attuale (numerico o percentuale);
- Il valore atteso da raggiungere (target di miglioramento);
- Le eventuali risorse e investimenti necessari;
- Il livello e la funzione organizzativa responsabile;
- La metodologia di misurazione, inclusi tempi, modalità di rilevazione e strumenti utilizzati.

La gerarchia e la struttura degli obiettivi è organizzata secondo una logica top-down, a partire dagli obiettivi strategici aziendali fino agli obiettivi operativi, garantendo allineamento tra visione strategica, governance del rischio e operatività quotidiana.

La Direzione assicura inoltre che:

- L'emissione del piano annuale degli obiettivi costituisce parte integrante della pianificazione del sistema;
- Le eventuali modifiche al SGSI, di natura organizzativa o documentale, siano pianificate e gestite in modo controllato all'interno del riesame della Direzione, in modo da non compromettere l'integrità e la coerenza del sistema stesso. Qualora emergano al di fuori di tale contesto, devono essere comunicate tempestivamente al Responsabile per la Sicurezza delle Informazioni (RSGSI), che ne valuta l'impatto e ne coordina l'attuazione riferendo alla Direzione.

7 SUPPORTO

7.1 RISORSE

L'organizzazione, nel rispetto della propria politica e dei propri obiettivi strategici, ha identificato le risorse indispensabili per:

- Attuare, mantenere e aggiornare efficacemente il SGSI, assicurandone la piena operatività in relazione ai processi, ai ruoli e alle misure di sicurezza implementate;
- Sostenere un percorso di miglioramento continuo del sistema, attraverso il potenziamento di strumenti, competenze, metodologie di gestione e tecnologie di protezione delle informazioni;
- Assicurare la disponibilità costante di risorse tecniche, economiche, infrastrutturali e umane, al fine di garantire il raggiungimento degli obiettivi di sicurezza e la risposta adeguata a eventuali nuove esigenze, rischi emergenti o modifiche significative del contesto operativo.

La valutazione dell'adeguatezza e disponibilità delle risorse è condotta regolarmente in sede di Riesame della Direzione, che rappresenta il momento chiave per:

- Verificare la conformità del SGSI agli obiettivi stabiliti;
- Identificare eventuali necessità di adeguamento o potenziamento delle risorse;
- Pianificare interventi correttivi o migliorativi basati sull'analisi delle prestazioni, dei cambiamenti del contesto o delle esigenze espresse dalle parti interessate.

Al fine di assicurare che le persone, nei diversi ruoli e responsabilità, agiscano con competenza e consapevolezza nell'ambito delle proprie mansioni, l'organizzazione ha implementato un approccio strutturato alla gestione risorse, che prevede:

- La valutazione iniziale e periodica delle conoscenze, esperienze e capacità del personale interno, con particolare attenzione alle funzioni che influiscono sulla sicurezza delle informazioni;
- L'organizzazione di programmi formativi mirati, rivolti sia al personale neoassunto sia a quello già in organico, con lo scopo di garantire l'acquisizione e l'aggiornamento delle competenze necessarie in relazione ai ruoli assegnati;

- L'addestramento specifico per mansioni critiche, soprattutto per i processi che gestiscono informazioni classificate, sensibili o soggette a requisiti normativi stringenti;
- Il mantenimento di registrazioni aggiornate relative ai percorsi formativi, ai partecipanti, ai contenuti trattati e ai livelli di competenza raggiunti, in modo da assicurare la tracciabilità e la verifica dell'efficacia delle azioni formative.

Le attività di formazione e sensibilizzazione sono pianificate annualmente, su proposta della Direzione, in base alle esigenze emerse dal contesto aziendale, dai risultati delle valutazioni del rischio, dagli esiti delle verifiche interne e dai cambiamenti normativi o tecnologici che impattano sulla sicurezza delle informazioni.

TRANSTEC SERVICES S.R.L. garantisce che tutte le attività legate alla sicurezza delle informazioni siano condotte in ambienti fisici idonei, sicuri e conformi alle normative vigenti in materia di protezione dei dati e di salute e sicurezza sul lavoro.
Nell'ambito della pianificazione dei processi aziendali e durante i Riesami della Direzione, l'organizzazione valuta in modo sistematico l'adeguatezza di:

- Strutture e ambienti di lavoro, tra cui locali ad uso ufficio nei quali si svolge attività amministrativa e gestionale
- Adeguata disponibilità di apparecchiature, attrezzature, dispositivi hardware e software per lo svolgimento delle attività riguardanti lo scopo dell'organizzazione.
- Servizi ausiliari e infrastrutture di supporto, essenziali per garantire la disponibilità e l'integrità delle informazioni.

L'organizzazione adotta tutte le misure necessarie affinché gli ambienti di lavoro:

- Siano mantenuti in condizioni sicure, ordinate e adeguate al tipo di attività svolta;
- Dispongano di regole operative e istruzioni per la gestione sicura delle informazioni e delle infrastrutture;
- Sostengano il benessere organizzativo, la collaborazione tra le persone e la motivazione del personale, riconoscendo che questi fattori contribuiscono indirettamente alla protezione efficace delle informazioni.

Per garantire l'affidabilità delle attrezzature impiegate nei processi critici del SGSI, TRANSTEC SERVICES S.R.L. ha attuato un programma di manutenzione

programmata, con registrazioni tracciabili, al fine di prevenire guasti o malfunzionamenti che possano compromettere la sicurezza delle informazioni.
Tutti gli asset fisici e informatici rilevanti per la sicurezza delle informazioni sono censiti, classificati e gestiti secondo quanto stabilito nel Registro degli Asset Aziendali, che include anche i criteri di manutenzione, protezione e controllo dell'accesso fisico.
In particolare, per quanto riguarda la protezione dei dati digitali, l'organizzazione applica politiche e procedure documentate per garantire:

- L'esecuzione regolare di backup automatici e sicuri, secondo piani approvati e monitorati dal Responsabile per la Sicurezza delle Informazioni (RSGSI);
- Il ripristino tempestivo dei dati in caso di incidenti o interruzioni;
- La protezione fisica e logica dei sistemi di backup, anche tramite meccanismi di cifratura, replica geografica e conservazione ridondata.

Nel caso di acquisizione di nuove attrezzature critiche, soggette a manutenzione o rilevanti per la sicurezza delle informazioni, l'azienda provvede a:

- Effettuarne la registrazione nel sistema di gestione degli asset;
- Pianificare e documentare le attività di manutenzione preventiva e correttiva;
- Verificare la conformità tecnica e di sicurezza delle nuove risorse prima dell'integrazione operativa.

Queste misure assicurano che le condizioni ambientali e infrastrutturali supportino in modo efficace il funzionamento sicuro, conforme e continuo del SGSI.

7.2 COMPETENZE

L'identificazione delle competenze è parte integrante della pianificazione del SGSI e si basa sull'analisi dei requisiti specifici di ciascun processo, garantendo che tutte le attività con impatto sulla sicurezza delle informazioni siano gestite da personale adeguatamente qualificato.
Per ogni profilo professionale aziendale sono valutati e documentati i seguenti ambiti di competenza:

- Competenze gestionali, ossia la capacità di pianificare, coordinare, comunicare, negoziare e monitorare l'uso di risorse (umane, tecniche,

infrastrutturali, economiche) ai fini del raggiungimento degli obiettivi di sicurezza delle informazioni.
- Competenze tecniche, riferite alla conoscenza e applicazione di normative, standard, tecnologie e metodologie specifiche della sicurezza delle informazioni.
- Competenze operative, ovvero l'abilità di eseguire attività pratiche e specifiche secondo procedure e protocolli predefiniti.

La metodologia adottata da TRANSTEC SERVICES S.R.L. per l'analisi delle competenze professionali prevede:

1. Identificazione dei ruoli chiave all'interno dei processi del SGSI;
2. Mappatura delle competenze attese per ciascun ruolo, in relazione ai rischi associati e alle attività critiche;
3. Valutazione delle competenze possedute da ciascun individuo tramite strumenti come schede di valutazione, colloqui tecnici e verifica dei titoli/esperienze;
4. Pianificazione di azioni formative, laddove si riscontrino scostamenti tra le competenze attese e quelle disponibili;
5. Verifica e aggiornamento periodico della matrice delle competenze, in base a cambiamenti organizzativi, tecnologici o normativi.

La gestione delle competenze è supportata da registrazioni documentate, che includono i requisiti di qualifica per ciascun ruolo, l'elenco dei corsi frequentati, i livelli di competenza raggiunti, le attività di aggiornamento continuo e l'eventuale bisogno formativo residuo.

L'organizzazione valuta costantemente il ritorno in termini di efficacia delle azioni intraprese per migliorare la sicurezza delle informazioni, misurando l'impatto del miglioramento delle competenze sulla gestione dei rischi e sulla protezione dei dati. In questo contesto, la formazione e l'addestramento non sono solo strumenti di compliance, ma anche leve strategiche per garantire l'eccellenza operativa, l'affidabilità del SGSI e il raggiungimento degli obiettivi aziendali.

Le attività di formazione e addestramento sono parte integrante del piano di sviluppo delle competenze e sono destinate a:

- Mantenere le competenze aggiornate per garantire che il personale sia sempre allineato con le normative in evoluzione e le best practices in materia di sicurezza delle informazioni;

- Sostenere il miglioramento continuo delle competenze professionali per l'efficace gestione del SGSI, in linea con gli obiettivi qualitativi e di soddisfazione del cliente stabiliti dall'azienda;
- Garantire la conformità alle prescrizioni legali e alle politiche interne aziendali.

In particolare, si distinguono due tipologie di attività formative:

- Attività di Formazione
  Le attività di formazione sono orientate principalmente alla trasmissione di conoscenze generali che, pur avendo un impatto ampio e trasversale, vengono successivamente contestualizzate e applicate all'interno dei processi aziendali specifici.
- Attività di Addestramento
  Le attività di addestramento sono orientate principalmente a sviluppare competenze pratiche e operative, che vengono acquisite direttamente sul posto di lavoro attraverso il cosiddetto on-the-job training. Queste attività sono condotte affiancando il personale a colleghi esperti o a consulenti esterni specializzati. Tali attività sono volte a garantire che le competenze siano immediatamente applicabili e che il personale possa gestire situazioni reali e scenari di emergenza.

7.3 CONSAPEVOLEZZA

L'organizzazione si occupa costantemente di svolgere attività di sensibilizzazione il cui obiettivo è garantire che tutti i soggetti coinvolti nei processi organizzativi comprendano i principi fondamentali della sicurezza delle informazioni, le proprie responsabilità e le conseguenze di eventuali comportamenti non conformi.

In particolare, i programmi di sensibilizzazione sono finalizzati a fornire conoscenza e consapevolezza riguardo a:

- Gli aspetti fondamentali della sicurezza delle informazioni e la loro integrazione nei processi aziendali, incluse le modalità con cui il SGSI è applicato operativamente;
- La politica aziendale per la sicurezza delle informazioni, gli obiettivi e i traguardi stabiliti dalla Direzione, le procedure operative, nonché tutti i requisiti cogenti o contrattuali applicabili al contesto dell'organizzazione;
- Le potenziali conseguenze gestionali, operative e legali derivanti da comportamenti non conformi alle disposizioni del SGSI, comprese

violazioni di sicurezza, perdita di dati, accessi non autorizzati o uso improprio di sistemi informativi;
- Le responsabilità individuali nella protezione delle informazioni, inclusi i doveri di riservatezza, l'adozione di buone pratiche di sicurezza e l'obbligo di segnalazione di eventuali anomalie, incidenti o rischi.

7.4 COMUNICAZIONE

TRANSTEC SERVICES S.R.L. ha strutturato un sistema efficace per la gestione delle comunicazioni interne ed esterne relative al Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), garantendo che tutte le parti interessate siano correttamente informate, coinvolte e aggiornate in merito agli aspetti critici della sicurezza delle informazioni.

Le comunicazioni possono essere di diversa natura e vengono gestite attraverso diversi canali ufficiali, tra cui:
- E-mail aziendale;
- Riunioni periodiche e dedicate;
- Comunicati interni, affissi in aree comuni o distribuiti digitalmente;
- Chiamate o incontri one-to-one, per casi urgenti o personalizzati;
- Eventuali strumenti aziendali di collaborazione (es. intranet, piattaforme di messaggistica aziendale);

Le comunicazioni riguardano tanto il flusso top-down (dalla Direzione al personale operativo) quanto quello bottom-up (dal personale verso la Direzione), al fine di stimolare un dialogo bidirezionale utile per la segnalazione di anomalie, suggerimenti, esigenze formative o rischi emergenti.

7.5 INFORMAZIONI DOCUMENTATE

La Direzione ha definito e diffuso un sistema strutturato per la gestione della documentazione all'interno del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), assicurando che tutte le informazioni documentate siano disponibili, aggiornate e protette. Tali documenti rappresentano lo standard operativo e organizzativo dell'azienda e costituiscono un riferimento fondamentale per il controllo delle attività.

La Direzione approva e autorizza la documentazione seguendo le modalità stabilite nelle procedure aziendali, garantendo che essa sia distribuita nei punti di utilizzo, rimossa quando obsoleta e aggiornata secondo le necessità.
I documenti vengono creati e gestiti in modo che siano facilmente identificabili e accessibili a chi ne ha bisogno. Qualsiasi modifica è soggetta allo stesso processo di approvazione previsto per la prima emissione e viene tracciata in modo trasparente tramite tabelle di revisione presenti sui documenti stessi. L'elenco delle emissioni è costantemente aggiornato per assicurare l'utilizzo esclusivo delle versioni in vigore.
Anche la documentazione esterna, come norme, leggi o regolamenti tecnici, è soggetta a controllo. La Direzione si occupa di verificarne la validità e di distribuirla al personale interessato, mentre il RSGSI ne gestisce la registrazione e l'archiviazione.
Le registrazioni, intese come evidenza oggettiva del funzionamento e dei risultati del SGSI, seguono le stesse modalità di gestione dei documenti principali. Sono conservate in modo controllato da personale incaricato, anche quando non coincide con chi li ha prodotti, e devono essere archiviate tempestivamente. Tali registrazioni sono essenziali per dimostrare la conformità ai requisiti del sistema e sono soggette a un periodo di conservazione definito, in linea con le normative vigenti e le politiche aziendali.
Attraverso questo approccio integrato e controllato, l'organizzazione garantisce che la documentazione, tanto interna quanto esterna, contribuisca in modo efficace al mantenimento dell'integrità, della riservatezza e della disponibilità del SGSI.

8 ATTIVITÀ OPERATIVE

8.1 PIANIFICAZIONE E CONTROLLI OPERATIVI

L'Azienda garantisce che la pianificazione, l'esecuzione e il controllo delle proprie attività siano svolti in modo strutturato e conforme ai principi definiti nella politica per la sicurezza delle informazioni. Questa coerenza è assicurata attraverso l'adozione di documenti che fanno parte integrante del Sistema di Gestione per la Sicurezza delle Informazioni, i quali permettono di gestire in

maniera efficace le interazioni tra i vari processi aziendali e di monitorarne le prestazioni.

Ogni attività espletata è tracciata e documentata con registrazioni conservate all'interno della specifica Scheda Cliente, che rappresenta il punto di raccolta delle evidenze relative al servizio fornito. In questo modo, l'organizzazione garantisce la continuità e la tracciabilità delle informazioni, a tutela della qualità e della sicurezza del servizio.

Per assicurare l'affidabilità delle prestazioni erogate, sono stati implementati controlli operativi che coprono diverse aree chiave. Particolare attenzione è riservata alla comunicazione con il cliente, alla corretta erogazione del servizio, ai tempi di risposta e di esecuzione, alla soddisfazione del cliente e al rispetto della riservatezza dei dati personali. Questi aspetti, ritenuti fondamentali per la continuità e la qualità del servizio, sono monitorati e valutati regolarmente, con l'obiettivo di attivare azioni di miglioramento continuo e di garantire il rispetto dei requisiti applicabili.

Attraverso tale approccio, l'azienda dimostra il proprio impegno nel mantenere un sistema efficace di gestione della sicurezza delle informazioni, che sia in grado di assicurare la qualità operativa e la fiducia dei clienti.

8.2 VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

L'organizzazione ha stabilito un approccio strutturato per la valutazione periodica del rischio, volto a garantire la continua adeguatezza, efficacia e resilienza delle misure di sicurezza adottate. La frequenza delle valutazioni del rischio viene determinata in base ai seguenti criteri:

1. Valutazione periodica programmata
   La valutazione del rischio viene effettuata con cadenza almeno annuale, in coincidenza con il riesame della direzione. Questo consente di riesaminare i rischi in modo sistematico e coerente con le strategie e gli obiettivi aziendali, anche in assenza di eventi straordinari o non conformità.
2. A seguito di non conformità
   Una nuova valutazione del rischio viene condotta ogniqualvolta si verifichi una non conformità significativa, sia essa rilevata internamente

o esternamente. Tale azione ha lo scopo di individuare eventuali lacune nei controlli di sicurezza esistenti e aggiornare il trattamento del rischio in modo appropriato.

3. Modifiche significative agli asset informativi
   Qualora si verifichino cambiamenti rilevanti a livello di asset aziendali – ad esempio, l'introduzione di nuove tecnologie, infrastrutture, applicazioni critiche o processi – viene eseguita una rivalutazione dei rischi per garantire che i controlli di sicurezza siano adeguati al nuovo perimetro operativo.
4. Cambiamenti nel contesto organizzativo o esterno
   La valutazione del rischio viene altresì aggiornata in caso di modifiche significative al contesto interno (ad esempio: variazioni nella struttura organizzativa, strategie, acquisizioni) o al contesto esterno (ad esempio: evoluzione normativa, nuove minacce cyber, cambiamenti geopolitici o economici). Ciò assicura che il SGSI sia costantemente allineato con l'ambiente in cui opera l'organizzazione.

8.3 TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

L'organizzazione ha sviluppato e implementato un piano di trattamento del rischio per la sicurezza delle informazioni, con l'obiettivo di mitigare i rischi identificati e garantire la protezione adeguata delle informazioni sensibili. Il piano viene riesaminato regolarmente e aggiornato secondo le seguenti modalità:

1. Riesame annuale in occasione del riesame della direzione
   Il piano di trattamento del rischio è soggetto a una revisione annuale, che avviene come parte del riesame della direzione, al fine di valutare l'efficacia delle azioni di trattamento intraprese e verificare che le misure di sicurezza siano ancora adeguate rispetto agli obiettivi di sicurezza delle informazioni. Tale riesame si effettua anche in assenza di non conformità, per garantire la continuità e la coerenza del trattamento del rischio con le strategie aziendali.
2. A seguito di non conformità
   In caso di identificazione di una non conformità rilevante, sia essa derivante da audit interni, audit esterni o segnalazioni, il piano di

trattamento del rischio viene tempestivamente riesaminato e aggiornato. L'obiettivo è correggere le lacune riscontrate e adottare misure correttive appropriate per evitare il ripetersi delle non conformità, rafforzando così i controlli di sicurezza.

3. Modifiche significative agli asset aziendali
   Qualora si verifichino modifiche sostanziali agli asset aziendali, come l'introduzione di nuove tecnologie, sistemi o processi critici, il piano di trattamento del rischio è aggiornato per riflettere i nuovi rischi associati a tali cambiamenti. L'attuazione di nuovi asset comporta una valutazione del rischio per assicurare che i controlli di sicurezza siano efficaci e mirati alla protezione degli asset appena acquisiti o modificati.
4. Cambiamenti nel contesto organizzativo o esterno
   Ogni volta che si verificano cambiamenti significativi nel contesto interno (ad esempio modifiche nella struttura organizzativa, politiche aziendali o modifiche nella governance) o nel contesto esterno (quali nuove minacce informatiche, evoluzione delle normative, variazioni del mercato o condizioni economiche), il piano di trattamento del rischio viene riesaminato e adattato. L'organizzazione garantisce così che il trattamento del rischio continui a rispondere alle nuove sfide e condizioni operative.

Il piano di trattamento del rischio è un documento dinamico e in continua evoluzione, che viene costantemente monitorato, aggiornato e migliorato in base ai risultati del riesame, alle modifiche identificate e ai cambiamenti che potrebbero influenzare la sicurezza delle informazioni.
Tutti i riesami e gli aggiornamenti del piano di trattamento sono documentati e approvati da parte della direzione, assicurando che le decisioni siano basate su valutazioni accurate e tempestive.

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE

TRANSTEC SERVICES S.R.L. pianifica e attua processi strutturati di monitoraggio, misurazione, valutazione, analisi e miglioramento per garantire che il Sistema di Gestione per la Sicurezza delle Informazioni sia conforme ai

requisiti specificati e continui a migliorare nel tempo. Gli obiettivi principali di tali attività sono:

1. Dimostrare la conformità dei servizi erogati ai requisiti di sicurezza delle informazioni.
2. Assicurare la conformità e l'efficacia del SGSI nel suo complesso.
3. Migliorare continuamente l'efficacia del SGSI, al fine di garantire che il sistema resti adeguato ed efficiente rispetto agli obiettivi aziendali e alle minacce emergenti.

I risultati ottenuti vengono analizzati in modo complessivo e critico durante il riesame periodico della Direzione, al fine di garantire che tutte le azioni correttive e i miglioramenti necessari siano tempestivamente attuati. Questo processo di riesame garantisce che il SGSI rimanga efficace e allineato con le esigenze e le sfide aziendali.

L'organizzazione implementa i seguenti processi di misurazione, analisi e miglioramento:

- Viene svolta un'analisi continua dei processi e un monitoraggio dei risultati per garantire che il SGSI soddisfi i requisiti di sicurezza delle informazioni stabiliti. Questo monitoraggio viene effettuato anche tramite la revisione del piano degli obiettivi di sicurezza delle informazioni.
- La direzione esegue il riesame periodico del SGSI, monitorando l'avanzamento rispetto agli obiettivi di sicurezza predefiniti e decidendo le azioni correttive necessarie. L'efficacia del sistema viene migliorata anche attraverso l'analisi delle performance complessive.

I metodi di analisi utilizzati dall'organizzazione possono includere tecniche statistiche avanzate, come calcoli, diagrammi e istogrammi, per monitorare e analizzare i dati relativi alla conformità e alle performance del SGSI. Questi dati vengono riportati nei rapporti di riesame del SGSI e utilizzati come input per il processo decisionale della Direzione. L'uso di tecniche statistiche è fondamentale per garantire una visione chiara e consapevole delle prestazioni nel tempo, consentendo una gestione proattiva delle risorse e dei rischi.

Sono considerate necessità strategiche per il miglioramento continuo le seguenti attività di rilevazione e analisi:

- Analisi delle non conformità.

- Analisi dei reclami.
- Analisi degli incidenti.
- Analisi delle azioni correttive e delle azioni di miglioramento.
- Rilevazioni relative ai fornitori.

Queste informazioni sono utilizzate per:

- Dimostrare la conformità dei servizi rispetto ai requisiti di sicurezza delle informazioni
- Assicurare la conformità ed efficacia del SGSI attraverso l'analisi dei dati e delle performance.
- Verificare il successo della pianificazione delle attività di sicurezza delle informazioni.
- Valutare le prestazioni dei processi e dei fornitori esterni, per garantire che gli stessi soddisfino i requisiti di sicurezza e le performance attese.
- Individuare opportunità di miglioramento all'interno del SGSI, per adattarsi ai cambiamenti e alle nuove sfide.
- Verificare l'idoneità, l'adeguatezza e l'efficacia del SGSI, garantendo che il sistema rimanga funzionale e allineato alle necessità aziendali.

L'organizzazione ha individuato e definito i processi pertinenti all'interno del SGSI che devono essere monitorati e, ove applicabile, misurati. I processi vengono monitorati periodicamente per garantire che siano conformi agli obiettivi pianificati. Ogni processo è associato a specifici obiettivi misurabili, che includono:

- Identificazione del processo (es. gestione degli incidenti di sicurezza).
- Obiettivo per il processo (es. ridurre il tempo di risposta agli incidenti)
- Indicatore di misura attuale (es. tempo medio di risposta agli incidenti).
- Indicatore di misura obiettivo (es. tempo medio di risposta target)
- Identificazione delle risorse necessarie (es. formazione, strumenti tecnologici, etc.).
- Responsabilità per il raggiungimento dell'obiettivo (es. team di sicurezza IT).
- Metodologia di misurazione (come e quando misurare i progressi)

Qualora i risultati non siano raggiunti, vengono adottate tempestive azioni correttive per garantire che gli obiettivi vengano raggiunti. I progressi vengono monitorati e le eventuali azioni correttive vengono pianificate durante le riunioni di riesame della Direzione.

9.2 AUDIT INTERNI

Per garantire la corretta applicazione, il funzionamento e l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), nonché per verificare che i risultati siano in linea con quanto atteso e con la Politica per la Sicurezza delle Informazioni, l'organizzazione pianifica e attua audit interni.

La pianificazione degli audit interni avviene con cadenza annuale e comprende tutte le aree aziendali e tutti i punti del SGSI. La Direzione è responsabile della corretta applicazione del programma di audit, assicurandosi che venga rispettato e che le verifiche siano effettuate in modo completo ed efficace.
La programmazione degli audit viene effettuata tenendo conto dell'importanza che l'area o il processo da verificare riveste per la sicurezza delle informazioni. Vengono individuati i responsabili delle verifiche, garantendo che i verificatori siano competenti e imparziali.

I risultati degli audit sono documentati e comunicati ai responsabili delle aree verificate, i quali intraprendono azioni correttive tempestive per affrontare le carenze riscontrate durante gli audit. Gli audit interni sono anche utilizzati per verificare l'efficacia delle azioni correttive adottate in seguito a rilievi emersi durante visite precedenti.

I resoconti degli audit sono analizzati dalla Direzione durante il riesame periodico del SGSI, per valutare il rispetto delle normative e dei requisiti stabiliti. Durante le riunioni di riesame, vengono discussi i risultati degli audit e identificati eventuali miglioramenti o azioni da intraprendere.

Gli audit interni possono essere eseguiti utilizzando liste di controllo o seguendo le istruzioni di processo per garantire la sistematicità e la completezza delle valutazioni. Le osservazioni risultanti dagli audit vengono documentate nelle liste di riscontro o nei rapporti generati.

In alcuni casi, la Direzione può decidere di programmare ulteriori audit in base a particolari esigenze o situazioni emergenti che richiedano un approfondimento.

Il personale incaricato di eseguire gli audit (auditor) è selezionato dal Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RGSI) e deve possedere la competenza necessaria. Gli auditor devono aver ricevuto formazione adeguata in valutazione interna e avere esperienza specifica nel campo della sicurezza delle informazioni. Gli auditor devono sempre mantenere imparzialità e obiettività, garantendo che le verifiche siano eseguite con la massima attenzione e correttezza.

L'organizzazione effettua audit interni a intervalli predefiniti per accertare la conformità del SGSI rispetto a quanto pianificato, con particolare attenzione anche ai processi strategici. Gli audit sono finalizzati a verificare che il SGSI:

1. Sia conforme a quanto pianificato, ai requisiti delle normative internazionali e ai requisiti stabiliti dall'organizzazione stessa.
2. Sia stato efficacemente implementato e mantenuto, fornendo alla Direzione le informazioni necessarie sui risultati e sulle azioni correttive adottate.
3. Gli audit interni vengono pianificati e attuati seguendo le linee guida generali per gli audit di sistemi di gestione, assicurando l'indipendenza e l'imparzialità del processo. I risultati degli audit interni contribuiscono al riesame del SGSI da parte della Direzione, come previsto dalla gestione e valutazione del sistema.

9.3 RIESAME DELLA DIREZIONE

Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) viene riesaminato periodicamente per garantirne l'idoneità, l'adeguatezza e l'efficacia nel tempo. Il riesame include anche la valutazione della necessità di cambiamenti al sistema, alla politica e agli obiettivi dell'organizzazione. Il riesame del SGSI avviene, di norma, con periodicità almeno annuale. Durante il Riesame, vengono esaminati i seguenti aspetti attinenti alla Sicurezza delle Informazioni:

- I risultati delle verifiche ispettive interne e delle valutazioni sul rispetto delle prescrizioni legali e di eventuali prescrizioni sottoscritte dall'organizzazione;

- Il monitoraggio delle prestazioni e il grado di raggiungimento degli obiettivi e dei traguardi stabiliti;
- La valutazione dei rischi e il relativo piano di trattamento;
- Lo stato delle azioni preventive e correttive adottate;
- Le azioni susseguenti ai precedenti riesami da parte della Direzione;
- Le raccomandazioni per il miglioramento continuo;
- Gli effetti derivanti da cambiamenti, comprese modifiche alle prescrizioni legali e alle prescrizioni sottoscritte dall'organizzazione;
- Lo stato delle attività relative alla gestione delle risorse;
- Le comunicazioni provenienti dalle parti interessate, comprese le segnalazioni e i reclami dei clienti;
- Le comunicazioni pertinenti provenienti da parti interessate interne all'organizzazione, inclusi i reclami;
- Il progresso nell'attuazione dei programmi di formazione.

Il verbale del Riesame formalizza l'oggetto della riunione, includendo i partecipanti, i documenti esaminati, gli argomenti trattati e le azioni decise. Durante questo incontro vengono discussi i seguenti punti:

- Lo stato delle azioni derivanti dai precedenti riesami della Direzione
- I cambiamenti nei fattori esterni e interni che influiscono sul sistema di gestione per la sicurezza delle informazioni;
- Le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni, tra cui le non conformità e le azioni correttive intraprese, i risultati del monitoraggio e della misurazione, i risultati degli audit, il raggiungimento degli obiettivi per la sicurezza delle informazioni.

Gli elementi in uscita dal riesame comprendono decisioni relative a:

- Opportunità per il miglioramento continuo;
- Eventuali necessità di modifiche al sistema di gestione della sicurezza delle informazioni.

Tra le opportunità per il miglioramento continuo si possono individuare:

- La necessità di nuovi audit interni e di audit sui fornitori critici;
- La necessità di adottare opportune azioni correttive e preventive;
- La necessità di nuove risorse e piani di formazione;
- La revisione degli obiettivi di miglioramento del SGSI.

Il verbale del riesame e gli obiettivi di miglioramento vengono presentati in un incontro tra la Direzione e le funzioni interessate per esporre i contenuti discussi. Durante tale incontro possono essere effettuate modifiche agli obiettivi, previa approvazione della Direzione.
Il Verbale di Riesame costituisce una registrazione ufficiale del processo e delle decisioni prese.

10 MIGLIORAMENTO

10.1 NON CONFORMITÀ E AZIONI CORRETTIVE

Quando si verifica una non conformità, comprese quelle che emergono dai reclami, l'azienda è organizzata per:

- Reagire alla non conformità e, per quanto applicabile:
  - Intraprendere azioni per tenerla sotto controllo e correggerla;
  - Affrontarne le conseguenze;
- Valutare l'esigenza di azioni per eliminare la(e) causa(e) della non conformità, in modo che non si ripeta o non si verifichi altrove:
  - Riesaminando e analizzando la non conformità;
  - Determinando le cause della non conformità;
  - Determinando se esistono o potrebbero verificarsi non conformità simili;
- Attuare ogni azione necessaria;
- Riesaminare l'efficacia di ogni azione correttiva intrapresa;
- Aggiornare, se necessario, i rischi e le opportunità determinati nel corso della pianificazione;
- Effettuare, se necessario, modifiche al sistema di gestione per la sicurezza delle informazioni.
-

In caso di non conformità, l'azienda stabilisce se e quale azione correttiva o preventiva sia necessaria per eliminare le cause della non conformità. Ogni azione correttiva può essere intrapresa a seguito di:

- Emissione di uno o più rapporti di non conformità;
- Reclami e proteste dei clienti e del personale interno;
- Risultati di audit di prima parte o visite ispettive da parte di clienti;
- Risultati di verifiche ispettive da parte di organismi di certificazione;
- Riesami della Direzione;

- Segnalazioni da parte di terze parti;
- Attacchi esterni sui sistemi;
- Eventi incidentali che impattano sui sistemi informativi;
- Bug riscontrati sui software

È compito della Direzione, in seguito agli "input" descritti sopra, valutare e stabilire le necessità relative all'adozione di un'azione correttiva, analizzarne le cause e stabilire le modalità di attuazione, le responsabilità coinvolte nell'esecuzione e i termini dell'azione correttiva.

Il responsabile dell'area interessata all'azione correttiva ha il compito di eseguire o far eseguire le azioni necessarie, verificandone la corretta attuazione nei tempi stabiliti.

Ogni azione correttiva deve correggere efficacemente le cause di non conformità o di anomalia che l'hanno generata. La corretta esecuzione di un'azione correttiva e la valutazione dell'efficacia della stessa sono verificate al termine dei tempi indicati per l'attuazione. Una volta valutati i risultati, il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) chiude l'azione eseguita.

Nel caso in cui azioni correttive coinvolgano fornitori nella loro attuazione, questi vengono informati dell'inconveniente riscontrato e viene chiesto loro di comunicare l'azione correttiva che intendono adottare e le relative tempistiche. Tutte queste attività sono registrate in appositi documenti. In concomitanza con i riesami della Direzione, RSGSI raccoglie le azioni correttive periodiche e le sottopone all'attenzione della Direzione.

Le azioni preventive scaturiscono dalle attività di riesame da parte della Direzione, in seguito a valutazioni di risultati, riepiloghi analitici provenienti dalle diverse aree aziendali, in relazione a potenziali cause di non conformità. È compito della Direzione gestire le attività di definizione delle azioni preventive, individuandone le cause, e stabilire le modalità di attuazione, le responsabilità coinvolte e i termini temporali.

Ogni azione preventiva deve quindi essere intrapresa nei tempi stabiliti dal responsabile incaricato dell'esecuzione. Al termine dei tempi previsti per la sua

attuazione, l'azione effettuata è riesaminata dalla Direzione che ne valuta i risultati in relazione agli obiettivi stabiliti.

Queste attività sono tutte registrate in appositi documenti, che vengono poi consegnati a RSGSI. In concomitanza con i riesami della Direzione, RSGSI raccoglie le azioni preventive periodiche e le sottopone all'attenzione della Direzione.

10.2 MIGLIORAMENTO CONTINUO

La Direzione, in coerenza con la missione e la politica aziendale, ha la responsabilità di pianificare e gestire i processi necessari per il miglioramento continuo del sistema di gestione per la sicurezza delle informazioni. Di conseguenza, si struttura un sistema di gestione delle azioni di miglioramento.

Le Azioni di miglioramento adottate dall'organizzazione sono costituite da Azioni Correttive (AC) e Azioni Preventive (AP), che vengono attuate per migliorare e risolvere Non Conformità, prassi aziendali errate e/o non coerenti, anche potenzialmente, con la politica e gli obiettivi definiti dal vertice, per adeguarsi a segnalazioni e tendenze in arrivo dal mercato.

Le Azioni Correttive hanno un'ottica reattiva di risposta e risoluzione ad anomalie e non conformità in generale, mentre le Azioni Preventive consentono di agire in maniera proattiva, prima che si verifichino eventi potenzialmente problematici.

Caratteristica di entrambe, che le contraddistingue dalle azioni di correzione delle non conformità che si concentrano sull'eliminazione dell'effetto indesiderato, è che esse si concentrano, in maniera appropriata, sulle cause delle situazioni anomale o potenzialmente anomale, al fine di prevenirne il loro ripetersi.

Gli strumenti e i supporti da utilizzare per l'attività di gestione del miglioramento sono:

- la politica per la sicurezza delle informazioni e gli obiettivi formalizzati e misurabili,
- le registrazioni relative ai risultati delle verifiche ispettive interne,
- le registrazioni riferite all'analisi dei dati,

- le registrazioni circa la gestione delle non conformità e la gestione delle azioni correttive e preventive,
- i verbali di registrazione dei riesami della direzione.