MANUALE SULLA SICUREZZA DELLE INFORMAZIONI

In conformità ai requisiti della norma

UNI EN ISO/IEC 27001:2013
"Sistemi di gestione della sicurezza delle informazioni – Requisiti"

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Sommario

1. Scopo 4
1.1 L'azienda 4
1.2 Prodotti e servizi 5
1.3 Approccio per processi 6
1.4 Rappresentazione di un processo nel sistema 7
1.5 Pensiero basato sul rischio (Risk-Based Thinking) 7
1.6 Compatibilità ed integrazione con altri Sistemi di Gestione Aziendali 8
2. Norme di riferimento 9
3. Termini e definizioni 10
3.1 Abbreviazioni 13
3.2 Matrice requisiti applicabili ISO 27001:2017 - indice e requisiti applicabili – correlazione norme 14
4. Contesto Aziendale 16
4.1 Comprendere l'organizzazione e il suo contesto 16
4.2 Comprendere i bisogni e le aspettative delle parti interessate 17
4.3 Scopo del Sistema di Gestione per la Sicurezza delle Informazioni 18
4.4 Esclusioni 18
4.5 Sistema di Gestione per la Sicurezza delle Informazioni e suoi Processi 19
4.6 Il Manuale per la Sicurezza delle Informazioni 19
4.7 Le Procedure Sicurezza delle Informazioni 20
4.8 Norme Operative 21
4.9 Processi del Sistema di Gestione per la Sicurezza delle Informazioni 21
4.10 Procedure Sicurezza delle Informazioni di riferimento 23
5. Leadership 24
5.1 Leadership e Impegno 24
5.1.1 Leadership e impegno per il sistema di gestione per la Sicurezza delle Informazioni 24
5.2 Politica per la Sicurezza delle informazioni 24
5.3 Ruoli, responsabilità e autorità nell'organizzazione 25
6. Pianificazione per il sistema di gestione per la Sicurezza delle Informazioni 26
6.1 Azioni per affrontare rischi e opportunità 26
6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per il loro conseguimento 27
Pianificazione dei cambiamenti 28

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

7. Supporto 29
7.1 Risorse 29
7.1.1 Generalità 29
7.1.2 Persone 29
7.1.3 Ambiente per l'esecuzione dei processi 32
7.1.4 Conoscenza organizzativa 33
7.2 Competenza, formazione-addestramento e consapevolezza 33
7.3 consapevolezza 35
7.4 Comunicazione 37
7.5 Informazione documentata 38
7.5.1 Generalità 38
7.5.2 Creazione e aggiornamento 38
7.5.3 Controllo delle informazioni documentate 40
8. Attività operative 45
8.1 Pianificazione e controlli e operativi 45
8.2 Valutazione del rischio relativo alla sicurezza delle informazioni 45
8.3 Trattamento del rischio relativo alla sicurezza delle informazioni 45
9. Valutazione delle prestazioni 46
9.1 Monitoraggio, misurazione, analisi e valutazione 46
9.2 Audit interno 48
9.3 Riesame di direzione 49
10. Miglioramento 51
10.1 Generalità 51
10.2 Non conformità ed azioni correttive 51
10.3 Miglioramento continuo 53

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 1

1. SCOPO

L'azienda DOS Group SA ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni conforme ai requisiti alla norma UNI CEI EN ISO 27001:2017 per:

- Ottenere un vantaggio competitivo soddisfacendo i requisiti contrattuali dei propri clienti con particolare attenzione alla sicurezza delle loro informazioni
- Eseguire in modo imparziale l'identificazione, la valutazione e la gestione dei rischi dell'organizzazione, formalizzando al tempo stesso i processi, le procedure e la documentazione relativi alla sicurezza delle informazioni
- Dimostrare con imparzialità l'osservanza delle leggi e normative applicabili
- Dimostrare l'impegno dei responsabili aziendali per garantire la sicurezza delle informazioni
- Garantire il monitoraggio costantemente delle prestazioni aziendali e attivare le azioni di miglioramento necessarie.

Il presente Manuale della Sicurezza delle Informazioni illustra come l'azienda si fa carico dei requisiti indicati dalla norma UNI CEI EN ISO 27001:2017 e dai requisiti indicati dalle normative applicabili.

1.1 L'AZIENDA

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Siamo una società informatica a Mendrisio con oltre 18 anni di esperienza: offriamo soluzioni business IT, come gestione di infrastrutture e servizi informatici completi. Soluzioni Business di DOS GROUP SA: assistenza tecnica allo sviluppo di siti web & applicazioni mobile, progettazione di infrastrutture, realizzazione di soluzioni business per l'impresa.

Ragione sociale:	DOS GROUP SA
Sede legale:	VIA RIME 38 6850 MENDRISIO – SVIZZERA
Sede operativa:	VIA RIME 38 6850 MENDRISIO – SVIZZERA
CHE:	CHE-109.036.022
Tel.:	+41 91 630 20 11
Sito internet:	www.dos-group.com
E-mail:	info@dos-group.com

1.2 PRODOTTI E SERVIZI

L'ambito del campo di applicazione: "PROGETTAZIONE E REALIZZAZIONE DI APPLICAZIONI SOFTWARE E SISTEMI DI EMERGENZA" sono comprese le attività di Assistenza e manutenzione di sistemi informatici proprietari, il disaster recovery a supporto dei servizi aggetto del campo d'applicazione e la connettività delle reti nella sua complessità.

Servizi offerti dall'azienda:

Servizi informatici - Infrastruttura as a Service (IaaS) e Workplace management: soluzioni cloud o ibride, macchine virtuali, sistemi di managed backup, security e file sharing. DOS Group è in grado di fornire un servizio completo ed affidabile.

Sviluppo web & mobile Applicazioni Mobile - progettazione e sviluppo di app per Android ed iOS, utilizzando la metodologia Agile e progettazione di UX e UI. Con oltre 10 anni di esperienza siamo in grado di supportare completamente la vostra azienda su tutti i progetti di sviluppo.

Soluzioni elettriche - Offriamo servizi nel settore elettrico – telematico, sia civile che industriale: dalla consulenza all'implementazione di impianti, fino alla realizzazione di impianti telefonici, Smart Home e videosorveglianza.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

1.3 APPROCCIO PER PROCESSI

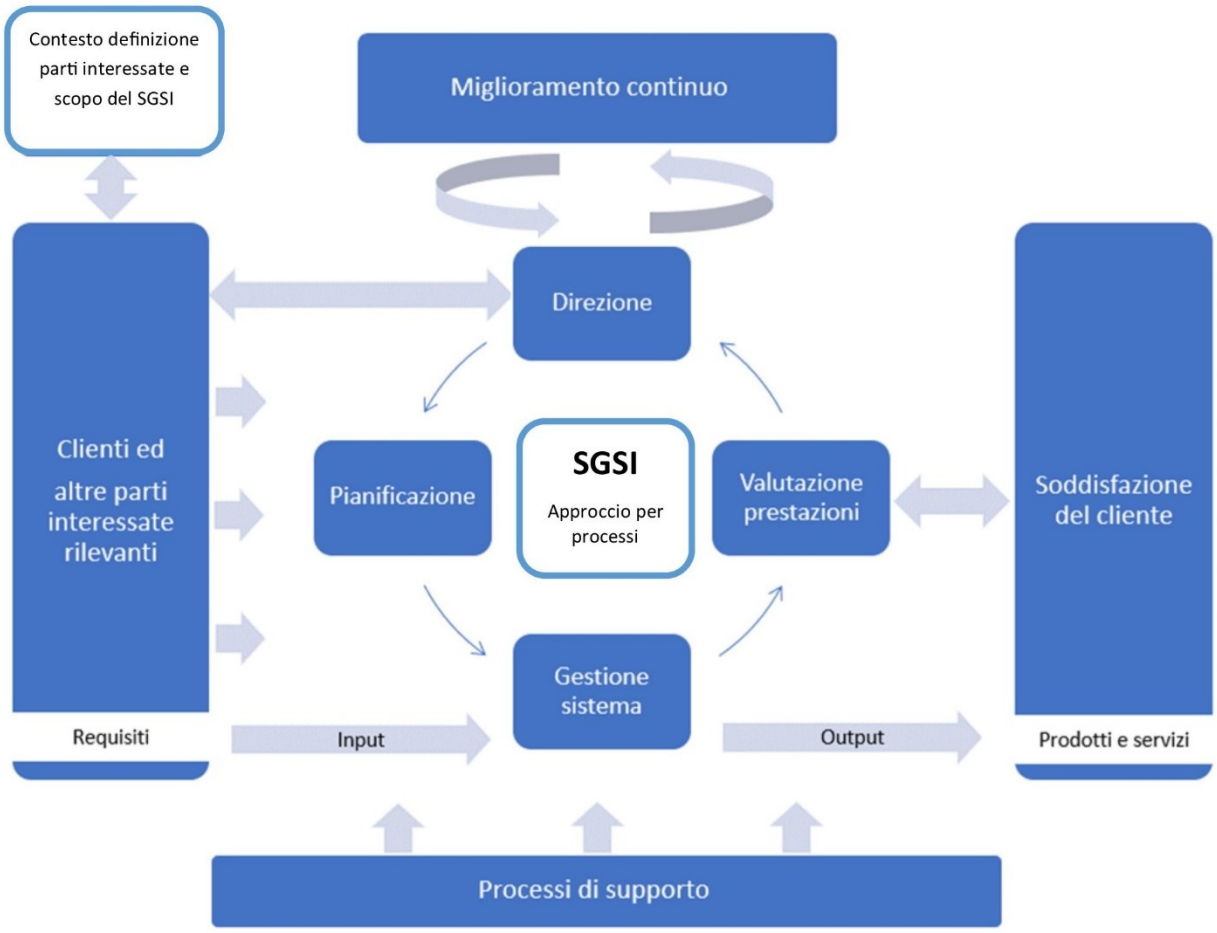
L'azienda DOS Group SA ritiene che i risultati previsti si raggiungano efficacemente ed efficientemente attraverso la gestione per processi.

La gestione per processi assicura:

- comprendere e soddisfare costantemente i requisiti;
- considerare i processi in termini di valore aggiunto;
- il raggiungimento di prestazioni efficaci dei processi;
- miglioramento del processo basato sulla valutazione dei dati e delle informazioni.

L'approccio per processi è applicato facendo ricorso alla metodologia PLAN-DO-CHECK-ACT con particolare attenzione al Pensiero Basato sul Rischio quale mezzo di prevenzione.

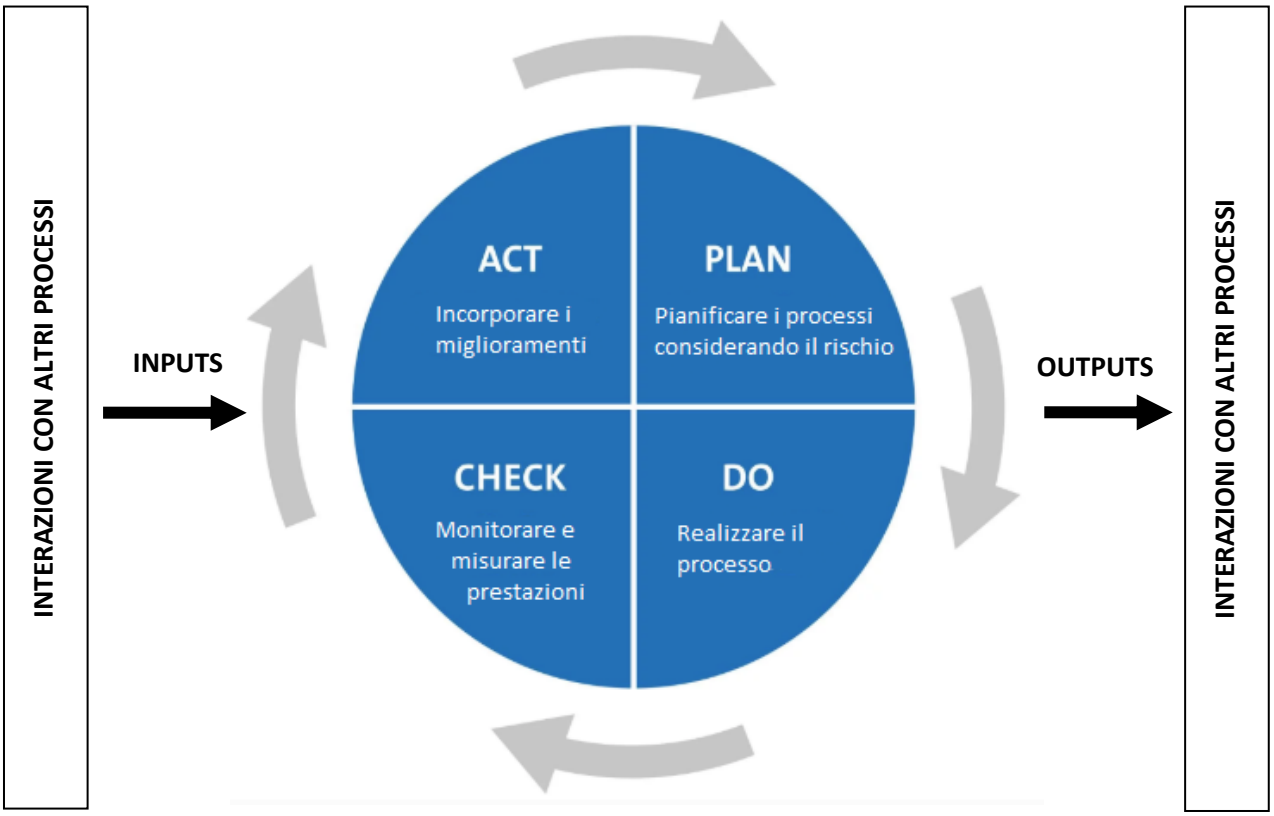
La figura che segue presenta graficamente il meccanismo di gestione dei processi:



Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

1.4 RAPPRESENTAZIONE DI UN PROCESSO NEL SISTEMA

Di seguito è rappresentato come un processo del sistema possa essere gestito attraverso il ciclo PLAN-DO-CHECK-ACT:



1.5 PENSIERO BASATO SUL RISCHIO (RISK-BASED THINKING)

L'effetto dell'incertezza di un determinato risultato ed il concetto di risk-based thinking, sono presi in considerazione nel Sistema di Gestione per la Sicurezza delle Informazioni dell'azienda DOS Group SA.
L'azienda considera tale concetto implicito e lo incorpora nei requisiti per stabilire, implementare, mantenere e migliorare continuamente il Sistema di Gestione per la Sicurezza delle Informazioni.
DOS Group SA adotta una particolare metodologia per l'adozione dell'approccio risk-based thinking basata anche sulla norma ISO 31000 che ne fornisce le linee guida.
L'azienda ha stabilito per ogni processo i livelli di rischio in termini di abilità dell'organizzazione nel raggiungere gli obiettivi fissati e le conseguenze sui processi, prodotti, servizi e non conformità di sistema.

Per l'azienda DOS Group SA "Risk-based thinking" significa considerare il rischio sulla Sicurezza delle Informazioni in modo dipendente dal contesto interno ed esterno dell'azienda.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Sono definiti il rigore ed il grado di formalità necessario per pianificare e controllare il Sistema di Gestione per la Sicurezza delle Informazioni, così come i suoi processi e attività.

1.6 COMPATIBILITÀ ED INTEGRAZIONE CON ALTRI SISTEMI DI GESTIONE AZIENDALI

L'azienda DOS Group SA ha adottato altri sistemi di gestione dei quali deve rispettare gli standard applicativi, altresì dovrà necessariamente rispettare molti requisiti previsti dalle normative in ambito di sicurezza del lavoro, e Privacy.

Per tale motivo la Direzione ha stabilito di integrare le attività cogenti relative alla sicurezza delle informazioni nei processi controllati dal presente Sistema di Gestione per la Sicurezza delle informazioni considerando i seguenti requisiti:

- Contesto aziendale
- Direzione, politica e responsabilità
- Processi per pianificare e considerare rischi ed opportunità
- Processi sulla sicurezza delle informazioni
- Processi di valutazione delle prestazioni
- Processi per il miglioramento

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 2

2. NORME DI RIFERIMENTO

L'azienda DOS Group SA 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
- UNI EN ISO 27001:2017 Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni
- UNI EN ISO 27002:2017 IT – Tecniche di sicurezza – Best Practices controlli di sicurezza
- UNI EN ISO 31000 Risk Management – Principi e linee guida

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

- Norme cantonali sulla riservatezza delle informazioni
- Norme cantonali sulla sicurezza del lavoro

Nota: I documenti di guida sono riportati solo nel Manuale; i documenti prescrittivi relativi all'attività di DOS Group SA sono riportati anche nell'**elenco documenti del SGSI** al quale si rimanda per l'altra documentazione di origine esterna.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 3

3. TERMINI E DEFINIZIONI

Si applicano le definizioni fornite dalla UNI EN ISO 9000:2015.

Nota: le definizioni riprodotte in modo identico dalle norme di riferimento o guida sono evidenziate con il simbolo (*)

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.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

I termini e le definizioni in materia di sistemi di gestione per la sicurezza delle informazioni sono definiti nella norma e UNI CEI EN ISO/IEC 27000:2017 (dizionario e vocabolario) a cui si rimanda per i termini e definizioni sulla sicurezza delle informazioni.

Riservatezza: proprietà per la quale le informazioni non siano rese disponibili o divulgate ad individui non autorizzati (ISO 27000 p.to 2.12).

Executive management: persona o gruppo di persone ai quali è stata delegata la responsabilità dall'organo di governo (2.29) per l'attuazione delle strategie e politiche atte a raggiungere l'obiettivo dell'organizzazione (ISO 27000 p.to 2.27).

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 (ISO 27000, p.to 2.33).

Continuità della sicurezza delle informazioni: processi/procedure atte a garantire continuità alla sicurezza delle informazioni (ISO 27000, p.to 2.34).

Incident 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 (ISO 27000, p.to 2.36).

Integrità: la proprietà di salvaguardare l'accuratezza e la completezza dei beni (ISO 27000, p.to 2.40).

Valutazione del rischio: processo globale di analisi del rischio e stima del rischio (ISO 27000, p.to 2.71).

Trattamento del rischio: processo di trattamento della scelta e dell'attuazione delle misure per modificare il rischio (ISO 27000, p.to 2.79).

Dichiarazione di applicabilità: dichiarazione documentata che descrive gli obiettivi del controllo e i controlli che sono pertinenti e applicabili al SGSI dell'organizzazione (ISO 27000, p.to 3.5.5 e).

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 catastrofi che potrebbero inficiare sul business continuità aziendale.

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

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

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, protetta 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

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

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.

Ai termini che seguono, ricorrenti nel presente manuale, onde evitare ambiguità, sono associate le definizioni indicate:

MGSI	Manuale per la Sicurezza delle Informazioni
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
BSI	Bacheca Sicurezza delle Informazioni
AC	Azione Correttiva
RGV	Responsabile gruppo di verifica
ODC	Organismo di certificazione
NC	Non Conformità

3.1 ABBREVIAZIONI

I titoli delle posizioni organizzative sono abbreviati come segue:

ACQ: Responsabile area Acquisti;

AMM: Responsabile area Amministrazione;

COMM: Responsabile area Commerciale;

DIR: Direzione;

IO: Istruzione Operativa;

M: Modulo o documento di registrazione;

CEO: Chief Executive officer

PS: Procedura Sicurezza delle Informazioni;

HR: Responsabile Risorse Umane;

RGSI: Responsabile Gestione Sicurezza delle Informazioni;

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

RIT: Responsabile Information Technology / IT Manager

SOA: Statement of Applicability.

RMRK: Responsabile area marketing / head of marketing

SA: Solution Architect

HR: Responsabile Risorse Umane;

RGSI: Responsabile Gestione Sicurezza delle Informazioni;

BO: Back office

SOA: Statement of Applicability.

RI: Responsabile infrastruttura Electrician and Telematic

VEN: Responsabile area vendite

ACQ: Responsabile area Acquisti

3.2 MATRICE REQUISITI APPLICABILI ISO 27001:2017 - INDICE E REQUISITI APPLICABILI – CORRELAZIONE NORME

	ISO IEC 27001:2017		Stato
0	Introduction	0	-
0.1	General	0.1	-
0.2	Compatibility with other management systems	0.6	-
1	Scope	1	-
2	Normative references	2	-
3	Terms and definitions	3	-
4	Context and organization	4	Applicato
4.1	Understanding the organization and its context	4.1	Applicato
4.2	Understanding the needs and expectations of interested parties	4.2	Applicato
4.3	Determining the scope of the information security management system	4.3	Applicato
4.4	Information security management system	4.4	Applicato
5	Leadership	5	Applicato
5.1	Leadership and commitment	5.1	Applicato
5.2	Policy	5.2	Applicato
5.3	Organizational roles, responsibilities and authorities	5.3	Applicato
6	Planning		Applicato
6.1.1	Actions to address risks and opportunities - general	6.1	Applicato
6.1.2	Information security risk assessment	-	Applicato

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

6.1.3	Information security risk treatment	-	Applicato
6.2	Information security objectives and planning to achieve them	6.2	Applicato
7	Support	7	Applicato
7.1	Resources	7.1	Applicato
7.2	Competence	7.2	Applicato
7.3	Awareness	7.3	Applicato
7.4	Communication	7.4	Applicato
7.5	Documented information	7.5	Applicato
8	Operation	8	Applicato
8.1	Operational planning and control	8.1	Applicato
8.2	Information security risk assessment	-	Applicato
8.3	Information security risk treatment	-	Applicato
9	Performance evaluation	9	Applicato
9.1	Monitoring, measurement, analysis and evaluation	9.1	Applicato
		9.1.1	Applicato
9.2	Internal Audit	9.2	Applicato
9.3	Management review	9.3	Applicato
10	Improvement	10	Applicato
10.1	Nonconformity and corrective action	10.2	Applicato
10.2	Continual improvement	10.3	Applicato

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 4

4. CONTESTO AZIENDALE

L'Azienda DOS Group SA ha determinato, verifica e riesamina costantemente quali problemi interni ed esterni possano avere effetti sull'effettiva capacità di fornire costantemente prodotti e/o servizi conformi ai requisiti del cliente e/o di leggi e regolamenti, ovvero sui risultati attesi dal Sistema di Gestione per la Sicurezza delle Informazioni.

4.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO

DOS Group SA ha determinato le questioni interne ed esterne pertinenti all'attività svolta e alla sua pianificazione strategica, che potrebbero in qualche misura influenzare la sua capacità di ottenere i risultati desiderati o attesi attinenti la Sicurezza delle informazioni.

Tra le questioni esterne da considerare, per quanto applicabile, a livello internazionale, nazionale, regionale e locale, si distinguono:

- ambiente legale
- ambiente tecnologico
- competitor
- mercato
- ambiente culturale, sociale ed economico
- giuridico

Tra le questioni interne da considerare, sempre per quanto applicabile, si distinguono:

- valori aziendali
- cultura e conoscenza
- prestazioni
- organizzativo
- fisico
- logico

DOS Group SA presenta il suo contesto nel documento "PS16 – *Analisi del contesto aziendale*" e nel documento "PS04B *Piano di valutazione dei rischi per la SI"* e ne analizza i cambiamenti e le questioni almeno una volta l'anno in sede di riesame della Direzione.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

4.2 COMPRENDERE I BISOGNI E LE ASPETTATIVE DELLE PARTI INTERESSATE

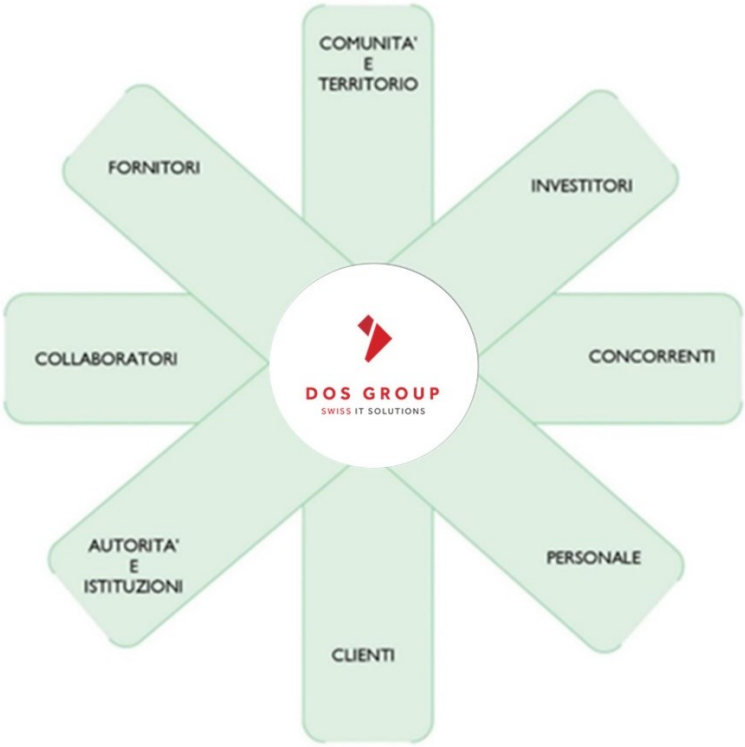
DOS Group SA ha individuato le parti interessate (stakeholders) che possono avere un impatto anche potenziale sulla capacità dell'organizzazione di fornire un servizio/prodotto conforme ai requisiti del Cliente e obbligatori applicabili e, per ciascuno di essi, ha determinato i requisiti pertinenti.

Tra le principali parti interessate, distinguiamo:

- proprietà
- clienti diretti
- fornitori e partner
- enti regolatori e Pubblica Amministrazione
- settore del credito
- ambiente
- lavoratori e collaboratori

Si rimanda per dettagli al documento *"*ALLEGATO A – *Mappa degli Stakeholders"* della PS16, in cui vengono chiaramente identificati i requisiti attesi (bisogni e aspettative ed i livelli di adeguatezza da minimo a buona pratica) di ciascuna parte interessata e relative misure e programmi intrapresi.

I requisiti definiti dalle parti (ad esempio regole del cliente, della PA, degli azionisti) vengono sistematicamente monitorati e riesaminati, almeno una volta l'anno in sede di riesame della Direzione.



Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

4.3 SCOPO DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Mediante lo sviluppo di un SGSI conforme ai requisiti delle norme UNI CEI EN ISO/IEC 27001:2017, l'organizzazione intende perseguire i seguenti obiettivi:

- tenere sotto controllo il contesto organizzativo nel quale opera;
- mantenere e migliorare la soddisfazione del cliente con riferimento alla conformità delle prestazioni erogate in termini di sicurezza delle informazioni;
- analizzare rischi e opportunità;
- mantenere e migliorare la solidità patrimoniale e la redditività aziendale;
- mantenere e migliorare la soddisfazione della proprietà con riferimento alla redditività ed alla stabilità degli assetti aziendali.

Il SGSI documentato dal presente manuale si applica alla norma UNI CEI ISO/IEC 27001:2017 per:

PROGETTAZIONE E REALIZZAZIONE DI APPLICAZIONI SOFTWARE E SISTEMI DI EMERGENZA

4.4 ESCLUSIONI

Tutti i requisiti della norma UNI CEI ISO/IEC 27001:2017 sono applicati. Per quanto concerne l'Annex, invece, risultano non applicabili i seguenti controlli:

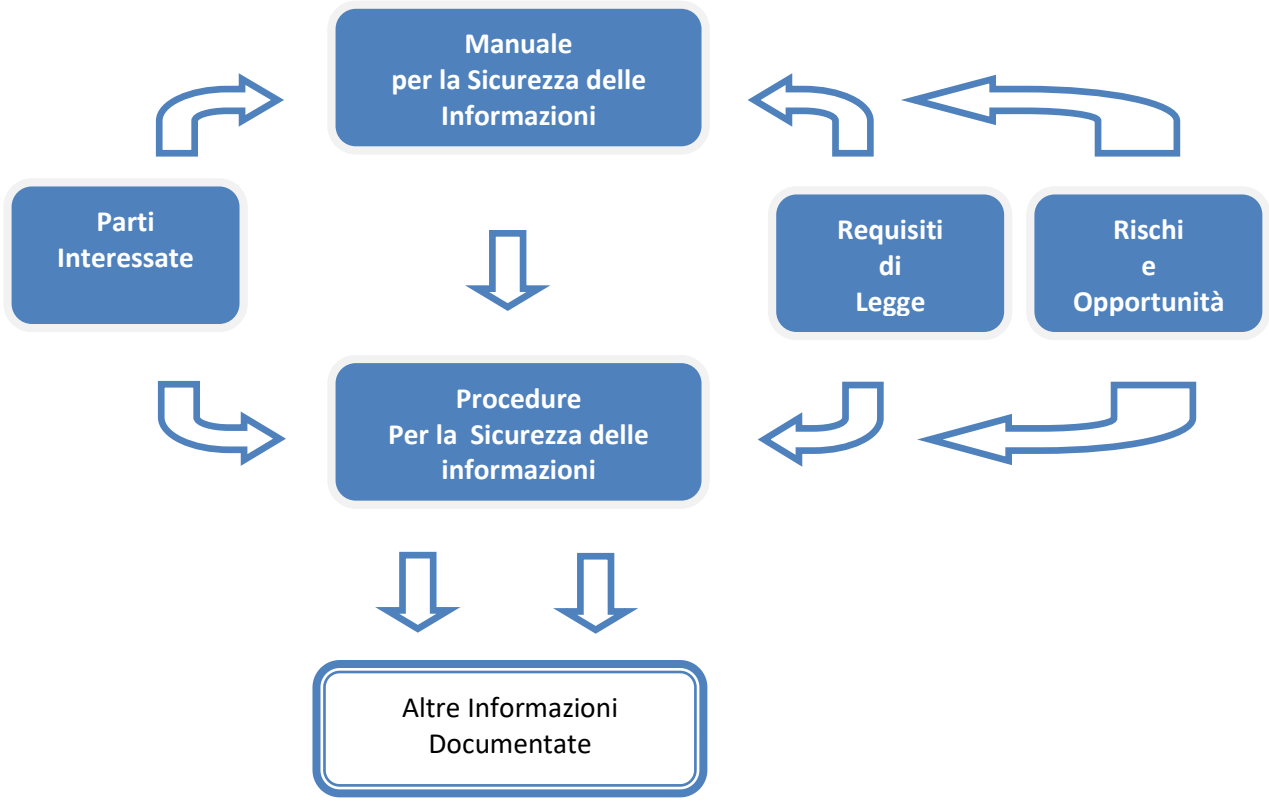
- A 6.2.2 Telelavoro

Il presente controllo è stato reso non applicabile in quanto l'azienda ha deciso di non dare la possibilità ai dipendenti, per motivi di sicurezza, di poter operare in telelavoro. Anche la figura giuridica e l'inquadramento dei contratti di lavoro non prevede tale tipo di opportunità.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

4.5 Sistema di Gestione per la Sicurezza delle Informazioni e suoi Processi

L'architettura della documentazione del Sistema è presentata con lo schema che segue.



4.6 Il Manuale per la Sicurezza delle Informazioni

Il Manuale per la Sicurezza delle Informazioni chiarisce la Politica Direzionale in materia di Sicurezza delle Informazioni; definisce l'approccio e le disposizioni generali relative ai processi aziendali aventi influenza sulla Sicurezza delle Informazioni descrivendo il campo di applicazione del sistema di gestione per la Sicurezza delle Informazioni con relative esclusioni. Alcuni capitoli del Manuale richiamano le Procedure per la Sicurezza delle Informazioni applicabili. In un apposito capitolo del presente Manuale SI è dato l'elenco delle procedure.

Nel Manuale per la Sicurezza delle Informazioni sono descritti:

- i processi del Sistema Sicurezza delle informazioni e la loro interazione
- i riferimenti alle PS;
- la politica direzionale in materia di Sicurezza delle Informazioni;

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

- regole relative alla Gestione della Sicurezza;
- regole per la conduzione delle valutazioni operate da terzi.

Il Manuale è costituito da:

- 1 pagina identificativa di copia,
- 2 pagine di indice dei capitoli,
- capitoli da 0 a 10.

Il Responsabile per la Sicurezza delle Informazioni trattiene tutte le copie del Manuale non diffuse.
Al momento della distribuzione il Responsabile della Sicurezza delle Informazioni identifica ogni copia distribuita, ne verifica la completezza e lo stato di aggiornamento, compila la pagina identificativa di copia e vi appone la propria sigla.
L'indice del manuale è siglato dalla D per approvazione.

Copie del Manuale sono diffuse internamente a:

n°1 Direzione
n°2 Ufficio RGSI

Tutte le copie sono gestite dal RGSI che provvede ad aggiornarle contemporaneamente in caso di modifica.
La distribuzione a soggetti esterni è autorizzata dal Responsabile per la Sicurezza delle Informazioni.
Tutte le copie interne sono soggette al servizio aggiornamento; il servizio è garantito dal Responsabile per la Sicurezza delle Informazioni.
Il contenuto delle revisioni è evidenziato in appositi paragrafi.

4.7 LE PROCEDURE SICUREZZA DELLE INFORMAZIONI

Le Procedure della Sicurezza delle Informazioni descrivono i processi richiesti per attuare il Sistema di Gestione per la Sicurezza delle Informazioni e comprendono:

- le Procedure sulla Sicurezza delle Informazioni che descrivono i processi e le attività necessarie per mettere in atto il sistema

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

- le Procedure sulla Sicurezza delle Informazioni che descrivono le sequenze e la natura interattiva dei processi rilevanti per garantire la conformità delle informazioni trattate nonché la loro integrità e sicurezza.

Le Procedure sulla Sicurezza delle Informazioni sono diffuse a tutte le persone che prendono parte alle attività indicate.
Ogni Procedura sulla Sicurezza delle informazioni può contenere, come parte integrante, allegati o moduli necessari alla tenuta sotto controllo del sistema di gestione.

4.8 NORME OPERATIVE

Altri documenti contenenti, o in cui registrare, informazioni documentate e che sono richiamati dal Manuale per la Sicurezza delle Informazioni e dalle Procedure sulla Sicurezza delle Informazioni sono piani, moduli e schede, check list; tutti strumenti necessari a descrivere come condurre determinate attività, nonché istruzioni che descrivono la pratica operativa e le attività di controllo dei processi.

4.9 PROCESSI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

La seguente tabella riporta o schema dei processi e la loro interazione:

Processo	Primario o di Supporto	Interno o Esterno	Interagisce con
Gestione Clienti	P	I	Gestione fornitori / Sviluppo attrezzature / Manutenzione
Gestione Fornitori	P	I	Lavorazioni esterne / Produzione / Gestione magazzino
Sviluppo e ricerca	P	I	Gestione Clienti / Erogazione Servizi
Erogazione dei servizi	P	I	Gestione Clienti / Gestione fornitori
Manutenzione	S	I	Erogazione servizi
Gestione asset	P	I	Gestione Fornitori / Servizi / Personale
Gestione personale	S	I	Tutti
Amministrazione	S	I/E	Tutti
Gestione Sistema per la Sicurezza delle informazioni	S	I	Tutti
Sistema Informatico	S	I	Tutti
Gestione documenti e registrazioni	S	I	Tutti
Riesame di Direzione	S	I	Tutti
Audit interno	S	I	Tutti
Gestione incident	S	I	Tutti

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Non conformità	S	I	Tutti
Azioni correttive	S	I	Tutti
Gestione reclami clienti	P	I	Tutti
Gestione ordini	P	I/E	Gestione clienti/ Erogazione servizi
Approvvigionamento	S	I	Gestione clienti/ Gestione fornitori/ Erogazione servizi
Processi operativi per la gestione dei servizi legati alla SI nell'applicazione del:. PROGETTAZIONE E REALIZZAZIONE DI APPLICAZIONI SOFTWARE E SISTEMI DI EMERGENZA.	P	I	Tutti
Controllo dispositivi di misurazione	S	E	Erogazione dei servizi
Gestione risorse infrastrutturali	S	I	Tutti
Sviluppo competenze risorse umane	S	I/E	Tutti

I processi sono descritti nelle Procedure per la Sicurezza delle Informazioni e per ognuno sono definiti:

- gli input richiesti e gli output attesi
- la sequenza e le interazioni dei processi
- i criteri, i metodi (incluse misurazioni e indicatori di prestazioni) e modalità di controllo dei processi
- le risorse necessarie e le modalità per garantire la loro disponibilità
- compiti e responsabilità assegnate
- rischi ed opportunità e piano di implementazione delle azioni per affrontarli
- metodi per monitorare, misurare e valutare i processi e, se necessario, le modifiche da adottare per raggiungere i risultati attesi
- opportunità per il miglioramento del processo e del sistema di gestione per la Sicurezza delle Informazioni.

Tutte le informazioni relative al funzionamento dei processi sono documentate e conservate come previsto nelle apposite procedure.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

4.10 PROCEDURE SICUREZZA DELLE INFORMAZIONI DI RIFERIMENTO

PS00 – Scopo

PS01 – Politica per la gestione della sicurezza delle informazioni

PS02 - Perimetro sicurezza informazioni

PS03 - Mappa delle informazioni

PS04A - Linee guida per la gestione del rischio

PS04B - Piano per la valutazione dei rischi per la sicurezza delle informazioni

PS05 - Dichiarazione di applicabilità

PS06A - Analisi del rischio

PS06B - Piano trattamento del rischio

PS07 - Processi di monitoraggio delle prescrizioni normative

PS09 - Controllo accessi

PS10 - Formazione, addestramento e sensibilizzazione

PS11 - Utilizzo delle dotazioni informatiche

PS12 – Tenuta sotto controllo dei documenti

PS13 – Tenuta sotto controllo delle registrazioni

PS14 – Audit Interno

PS15 – Gestione delle NC e AC

PS16 – Analisi del contesto aziendale

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 5

5. LEADERSHIP

5.1 LEADERSHIP E IMPEGNO

5.1.1 Leadership e impegno per il sistema di gestione per la Sicurezza delle Informazioni

L'Alta Direzione si impegna nello sviluppo e nella messa in atto del Sistema di Gestione per la Sicurezza delle Informazioni e nel miglioramento continuo della sua efficacia:

- comunicando all'organizzazione l'importanza di ottemperare ai requisiti del cliente ed a quelli cogenti applicabili;
- stabilendo la politica per la sicurezza delle informazioni;
- assicurando che la politica e gli obiettivi per la sicurezza delle informazioni siano stabiliti e siano compatibili con gli indirizzi strategici dell'organizzazione;
- effettuando i riesami da parte della Direzione;
- assicurando la disponibilità delle risorse necessarie al sistema di gestione per la sicurezza delle informazioni;
- promuovendo la consapevolezza dell'approccio per processi e il miglioramento continuo;
- coinvolgendo, guidando e sostenendo le persone affinché contribuiscano all'efficacia del sistema di gestione per la sicurezza delle informazioni;
- supportando gli altri pertinenti ruoli direzionali nel dimostrare la loro leadership, come applicabile nelle rispettive aree di responsabilità.

5.2 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Il presente capoverso riporta gli orientamenti della Direzione per la gestione della sicurezza delle informazioni rimandando a documenti più specifici ("policy") gli orientamenti applicabili a specifiche tematiche.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Per quanto attiene la Politica per la sicurezza delle informazioni si rimanda all'allegato "A2 - *Politica aziendale della sicurezza delle informazioni"* ed alla procedura "PS01 - *Politica per la gestione della sicurezza delle informazioni"* in ultima revisione.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

5.3 RUOLI, RESPONSABILITÀ E AUTORITÀ NELL'ORGANIZZAZIONE

La Direzione assicura che le responsabilità e le autorità sono definite e rese note nell'ambito dell'organizzazione definendo l'organigramma aziendale (rif. allegato B del MGSI) ed il mansionario (rif. allegato C del MGSI) che include:

a) definizione delle competenze e responsabilità;

b) caratteristiche e requisiti minimi (grado di istruzione, addestramento, abilità/caratteristiche personali ed esperienza, ecc.).

L'organigramma nominativo è reso noto all'interno dell'organizzazione attraverso rete intranet aziendale.

Organigramma e mansionario hanno il fine di:

- assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti delle norme UNI CEI EN ISO/IEC 27001:2017
- assicurare che i processi interagiscano e producano gli output attesi
- riferire alla Direzione in merito alle prestazioni del sistema di gestione ed ogni opportunità di miglioramento e necessità di cambiamento e innovazione
- assicurare la promozione della consapevolezza dei requisiti del cliente
- assicurare che l'integrità del SGSI sia mantenuta quando siano pianificati e messi in atto cambiamenti del SGSI.

A tale scopo, l'Alta Direzione ha designato, mediante lettera di nomina (rif. allegato D del MGSI), un Responsabile per la Sicurezza delle Informazioni (RGSI), che indipendentemente dalle altre sue responsabilità, supporta la Direzione nelle mansioni di cui sopra.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 6

6. PIANIFICAZIONE PER IL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

6.1 AZIONI PER AFFRONTARE RISCHI E OPPORTUNITÀ

Un approccio orientato alla pianificazione e alla gestione del rischio è essenziale ai fini della sicurezza delle informazioni. La pianificazione di DOS Group SA è espressa in procedure ed istruzioni che devono sempre prevedere sia le responsabilità delle attività da eseguire sia la sequenza delle attività stesse. Qualora tali procedure non fossero sufficienti al raggiungimento dei requisiti specificati o alla gestione del rischio verranno predisposti dei Piani specifici.

Inoltre, tutte le attività ed i relativi processi sono progettati (compreso il presente Manuale) secondo la logica PDCA (Plan – Do – Check – Act) al fine di avere un approccio di tipo preventivo, un controllo durante i processi ed una gestione dei segnali di ritorno, e tenendo conto anche dei rischi e opportunità che possono essere gestiti e intrapresi sempre nell'ottica della soddisfazione del cliente e conformità del servizio/prodotto.

Si rimanda per dettagli al modulo **Risk Analysis** ed alle procedure sicurezza sull'analisi dei rischi e relativi trattamenti allegate al sistema.

Per raggiungere gli obiettivi ed i requisiti di sicurezza delle informazioni periodicamente DOS Group SA si pone degli obbiettivi (vedere il modulo M6.2) che controlla per verificare il loro raggiungimento in sede di riesame della Direzione (M9.3), l'azienda si è dotata di una struttura tecnica e gestionale e di specifiche di servizio: questi fattori permettono una gestione della sicurezza delle informazioni dei servizi offerti.

I suddetti obiettivi sono espressi in modo quantificato, misurabile ed oggettivo e, se particolarmente complessi, sono previsti degli obiettivi intermedi.

Si sottolinea inoltre il fatto che nel Modulo "M6.2 - *Piano di miglioramento SI*" vengono chiariti, nel modo il più dettagliato possibile, le risorse impiegate per raggiungere i singoli obiettivi con chiaramente identificati le responsabilità e, ove possibile, gli obiettivi intermedi. Inoltre, vengono anche espressi i tempi per il raggiungimento degli obiettivi stessi, verificati da RGSI.

L'Alta Direzione mette a disposizione le risorse necessarie per la completa ed operativa attuazione del Sistema per la Sicurezza delle Informazioni, oltre a quelle necessarie per la gestione, esecuzione e verifica del lavoro, incluse le verifiche ispettive interne. Tali risorse sono analizzate in modo periodico in fase di riesame del sistema.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

DOS Group SA ha inoltre definito e documentato, in questo manuale, in procedure ed in istruzioni, come verranno soddisfatti i requisiti per la sicurezza delle informazioni, facendo sì che la pianificazione sia coerente con tutti i requisiti del sistema aziendale.

La pianificazione del Sistema di Gestione per la Sicurezza delle Informazioni, in questo modo, assicura che l'integrità del Sistema di Gestione sia conservata, quando anche siano attuate modifiche al sistema stesso.

6.2 OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI E PIANIFICAZIONE PER IL LORO CONSEGUIMENTO

Gli obiettivi per la sicurezza delle informazioni definiti dalla Direzione e condivisi attraverso adeguata comunicazione interaziendale con le funzioni responsabili pertinenti sono gestiti attraverso il modulo "M6.2 - *Piano di miglioramento SI*" e per ogni funzione, livello e processo.

La Direzione assicura, attraverso periodico monitoraggio in sede di riesame della Direzione, che gli obiettivi siano:

- coerenti con la politica per la sicurezza delle informazioni e aggiornati come appropriato
- pertinenti alla conformità di beni e servizi
- coerenti con i requisiti applicabili (del cliente e cogenti)

Nella pianificazione degli obiettivi, DOS Group SA ha determinato:

- le azioni da realizzare
- le risorse necessarie (umane, economiche e infrastrutturali)
- i responsabili
- i tempi di realizzazione
- i tempi e metodi di valutazione dei risultati.

La Direzione assicura che, per i pertinenti livelli e funzioni dell'organizzazione, siano stabiliti gli obiettivi per la sicurezza delle informazioni, compresi quelli necessari per ottemperare ai requisiti dei "prodotti/servizi".

Gli obiettivi per la sicurezza delle informazioni sono misurabili, gestiti in forma controllata e coerenti con la politica per la Sicurezza delle Informazioni.

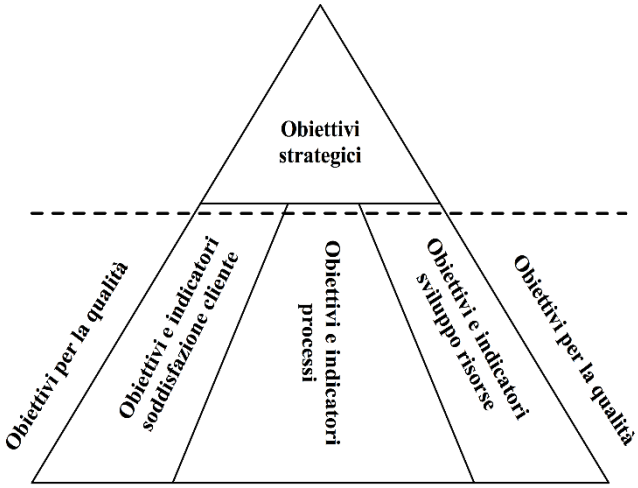
Tali obiettivi sono riportati nel "piano di miglioramento" (rif. mod. M6.2), emesso in sede di riesame della Direzione, e comprendente:

a) l'identificazione del processo;
b) l'obiettivo per quel processo;
c) l'indicatore di misura attuale (numerico o percentuale);
d) l'indicatore di misura che si vuol raggiungere (numerico o percentuale);
e) l'identificazione delle eventuali risorse/investimenti necessarie;
f) il pertinente livello/funzione dell'organizzazione responsabile del suo raggiungimento;

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

g) la metodologia di misurazione (ogni quanto e come) per il raggiungimento dell'obiettivo.

Nel diagramma sotto riportato è schematicamente rappresentata la gerarchia degli obiettivi aziendali.



La Direzione assicura che:

a) la pianificazione del SGSI è condotta in modo da ottemperare ai requisiti e conseguire gli obiettivi di cui sopra. L'emissione del piano degli obiettivi annuale, così come riportato al punto precedente, consente appunto di pianificare il SGSI ed i relativi processi;

b) le modifiche al SGSI (organizzative e documentali) sono pianificate ed attuate in modo controllato senza pregiudicarne l'integrità. Solitamente tali modifiche sono pianificate e verbalizzate nel riesame annuale da parte della Direzione. Eventuali modifiche decise al di fuori dal riesame della Direzione, sono comunicate al RGSI il quale assicura la loro pianificazione ed attuazione attraverso rapporti alla Direzione.

PIANIFICAZIONE DEI CAMBIAMENTI

Il sistema di gestione per la sicurezza delle informazioni deve essere continuamente riesaminato e, ove necessario, aggiornato apportando le opportune modifiche, che dovranno necessariamente essere condotte in modo pianificato e sistematico.

Per ciascuna proposta di cambiamento, la Direzione con le funzioni pertinenti dovranno considerare:

- lo scopo del cambiamento e le potenziali conseguenze (nell'ottica di potenziali rischi e opportunità)
- l'integrità del sistema di gestione per la sicurezza delle informazioni
- disponibilità di risorse
- allocazione e riallocazione di responsabilità e autorità, se necessario.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 7

7. SUPPORTO

7.1 RISORSE

7.1.1 Generalità

L'organizzazione ha individuato e rende disponibili le risorse necessarie per:

a) attuare e tenere aggiornato il SGSI;

b) accrescere e migliorare in modo continuo SGSI;

c) mettere a disposizione le risorse necessarie per quanto sopra delineato.

Tutto questo è attuato in uscita dal riesame della Direzione.

7.1.2 Persone

L'organizzazione ha stabilito il processo di gestione delle risorse umane attraverso un flusso definito nelle pagine seguenti. Tale processo permette che il personale che esegue attività che influenzano la conformità ai requisiti del prodotto/servizio, sia competente sulla base di un adeguato grado di istruzione, addestramento, abilità (caratteristiche personali) ed esperienza.

Il "mansionario aziendale" (rif. allegato C del MGSI) riporta:

a) la definizione delle competenze e responsabilità dell'organizzazione;

b) le caratteristiche ed i requisiti minimi (grado di istruzione, addestramento, abilità, caratteristiche personali ed esperienza).

Lo schema di flusso riportato di seguito rappresenta i criteri adottati di come l'organizzazione:

a) definisce la competenza necessaria per il personale che svolge attività che influenzano la sicurezza delle informazioni;

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

b) fornisce addestramento o intraprende altre azioni per soddisfare queste esigenze;

c) valuta l'efficacia delle azioni intraprese, assicura che il suo personale sia consapevole della rilevanza e dell'importanza delle proprie attività e di come esse contribuiscono al raggiungimento degli obiettivi per la sicurezza delle informazioni.

In funzione delle competenze necessarie, l'organizzazione definisce degli obiettivi di sviluppo delle competenze correlandoli agli obiettivi di soddisfazione dei clienti in termini di Sicurezza delle informazioni valutando quando i ritorni in termini di efficacia delle azioni intraprese.

In particolare si distingue tra:

- *attività di formazione*, ovvero attività che in genere prevedono lezioni in aula (interne o esterne all'azienda) e che sono essenzialmente mirate a trasmettere delle conoscenze di portata generale che devono poi essere calate nella specificità del caso concreto;
- *attività di addestramento*, ovvero attività che in genere sono svolte direttamente "on the job" mediante affiancamento a personale esperto (anche di origine esterna quali consulenti, esperti tecnici, ecc.).

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

c

Attività	Funzioni Coinvolte	Documenti
Input: necessità di risorse umane		
Individuazione necessità risorse umane	Direzione - RdF	Richiesta scritta, e-mail o verbale
Definizione delle competenze	RdF - HR	CV Mansionario
Esame richieste da parte della Direzione	Direzione	M9.3 – Riesame della Direzione
Valutazione risorse presenti	RdF - HR	CV Mansionario
Nuove risorse necessarie? (NO / SI)		
Ricerca impiego nuove risorse (selezione)	HR	CV
Addestramento personale per le mansioni necessarie	HR – RGSI - RdF	Piano della formazione Registro formazione interna
Impiego delle risorse umane identificate	Direzione – HR - RGSI	Lettera d'assunzione Zucchetti
Valutazione dell'efficacia dell'addestramento	HR – RGSI	Registro formazione interna
Formazione efficace? (NO / SI)		
Formazione/aggiornamento su SGI, politiche, obiettivi e valutazioni	RGSI – HR	M7.2 – Registro formazione interna
Formazione efficace? (NO / SI)		
Impiego di risorse umane competenti	RdF	
Output: disponibilità di risorse umane		

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Infrastrutture

L'organizzazione ha definito e messo a disposizione le infrastrutture necessarie per l'attuazione dei servizi richiesti.

L'organizzazione ha quindi individuato quali infrastrutture critiche per rispondere ai requisiti dei servizi forniti:

- le attrezzature e le apparecchiature utilizzate per l'erogazione dei servizi al fine di rispettare i programmi prefissati con il cliente;
- le strutture hardware e software utilizzate per la gestione informatizzata delle attività aziendali;
- gli immobili utilizzati dalla società.

L'organizzazione, inoltre, ha garantito l'assegnazione e la funzionalità dei dispositivi antincendio.

7.1.3 Ambiente per l'esecuzione dei processi

DOS Group SA è conforme alle vigenti normative riguardanti il rispetto della sicurezza delle informazioni e della salute dei lavoratori sul luogo di lavoro.

Durante la pianificazione dei processi, ed i riesami della Direzione sono valutate periodicamente le strutture ed i luoghi di lavoro, i materiali, gli strumenti, le attrezzature ed i servizi ausiliari.

L'organizzazione si adopera affinché gli ambienti di lavoro garantiscano condizioni ambientali ottimali, in conformità ai requisiti stabiliti, provvedendo a dotarli di appropriate attrezzature per il personale e assicurando la presenza di regole e guide per la sicurezza.

L'organizzazione si è inoltre adoperata perché gli ambienti di lavoro favoriscano le interazioni sociali e lo sviluppo delle potenzialità del personale, aumentandone la soddisfazione e la motivazione e migliorando, di conseguenza, le prestazioni dell'organizzazione.

Viene effettuata regolare manutenzione sulle attrezzature che necessitino di essere mantenute con cadenza programmata. Per quanto attiene la tenuta sotto controllo si rimanda al registro asset aziendali.

Per il salvataggio dei dati informatici, viene eseguito sistematico backup come da procedura prevista all'interno per la protezione delle informazioni.

Nel caso dovesse provvedere all'acquisto di attrezzature soggette a manutenzione, si provvederà a gestirle in maniera controllata attraverso adeguata registrazione delle stesse e di pianificazione delle attività di manutenzione.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

7.1.4 Conoscenza organizzativa

DOS Group SA considera i suoi collaboratori una risorsa strategica per il suo successo; per questo presta particolare attenzione alla conoscenza e sviluppo delle risorse umane, con una visione di formazione permanente e di crescita professionale, motivazionale e culturale di tutti i collaboratori di ogni livello e mansione.

DOS Group SA deve tener conto, nell'affrontare le mutevoli esigenze e tendenze, la propria conoscenza attuale e determinare modalità di accesso alle conoscenze aggiuntive necessarie che possono comprendere le proprietà intellettuali e gli insegnamenti derivanti dall'esperienza.

Per acquisire la conoscenza richiesta, l'organizzazione prende in considerazione:

- esperienze precedenti
- normative
- fonti accademiche
- conoscenze raccolte con i clienti o i fornitori.

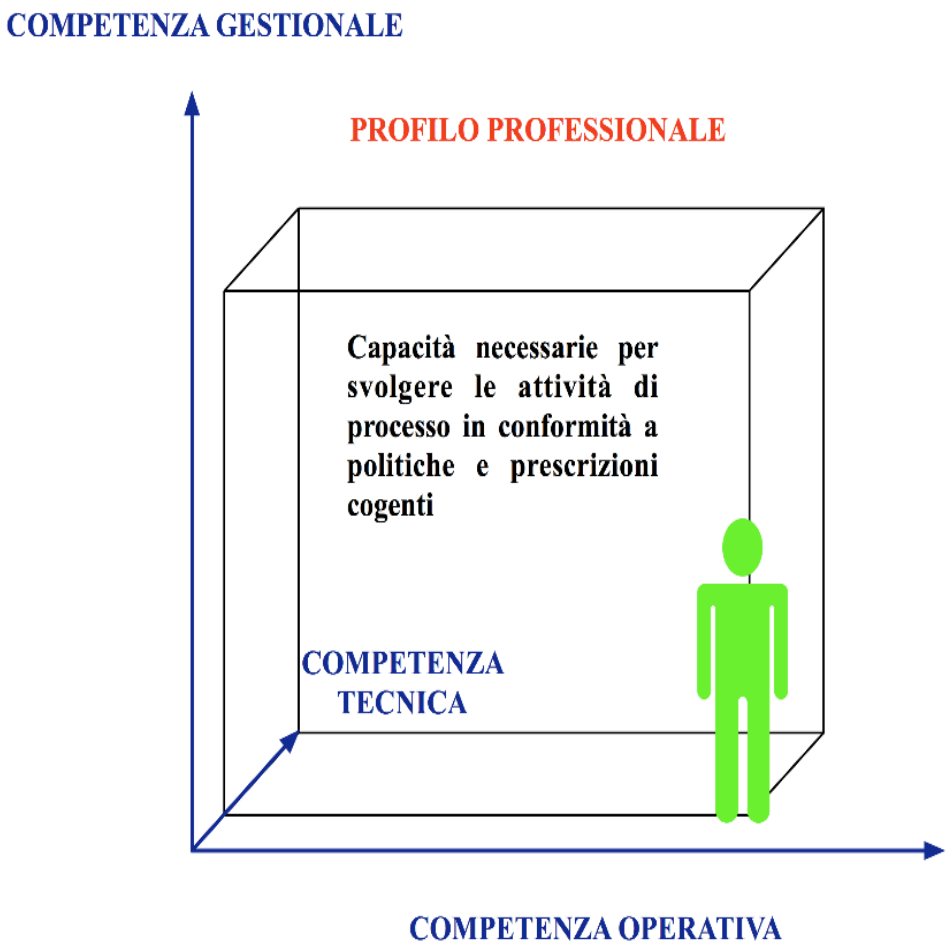
7.2 COMPETENZA, FORMAZIONE-ADDESTRAMENTO E CONSAPEVOLEZZA

L'Azienda definisce le competenze professionali richieste alle varie figure aziendali (attori del processo) al fine di assicurare la corretta attuazione del SGSI pianificato con particolare riferimento agli specifici processi in cui il SGSI stesso si articola. Il mix di competenze professionali richieste alla singola figura aziendale (profilo professionale) sono analizzate in funzione della loro natura:

- *competenze di natura gestionale*, ovvero la capacità di gestire (pianificare, programmare, negoziare, comunicare, coordinare, ecc.) risorse (umane, infrastrutturali, economiche, ecc.) per il conseguimento di determinati obiettivi;
- *competenze di natura tecnica*, ovvero la capacità di applicare conoscenze di carattere generale (conoscenza scientifica, conoscenza giuridica, conoscenza tecnica, ecc.) al caso specifico per ottenere determinati risultati;
- *competenze di natura operativa*, ovvero la capacità di svolgere determinate operazioni, utilizzando determinati strumenti, in conformità a procedure e ad istruzioni predefinite.

Nello schema sotto riportato viene schematicamente illustrata la metodologia di analisi delle competenze professionali in materia di sicurezza delle informazioni.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.



Ogni processo strategicamente rilevante viene pianificato per quanto concerne le competenze necessarie degli attori di processo in modo da meglio focalizzare le necessarie azioni di intervento e da facilitare la comunicazione al personale stesso della diretta conseguenza delle proprie attività sulla prestazione erogata dal processo.

In funzione delle competenze necessarie l'Azienda definisce degli obiettivi di sviluppo delle competenze correlandoli agli obiettivi di soddisfazione dei clienti e di qualità dei processi e valutando quindi in tal modo i ritorni in termini di efficacia delle azioni intraprese a copertura della sicurezza delle informazioni.

Le attività di formazione e di addestramento sono finalizzate, inoltre, a mantenere e a sviluppare le competenze delle figure professionali aziendali al fine di supportare il mantenimento e lo sviluppo del SGSI. Questo in funzione delle prescrizioni di legge e delle politiche qualitative definite dall'Azienda. In particolare si distingue tra:

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

- *attività di formazione*, ovvero attività che in genere prevedono lezioni in aula (interne o esterne all'Azienda) e che sono essenzialmente mirate a trasmettere delle conoscenze di portata generale che devono poi essere calate nella specificità del caso concreto. Annualmente l'Azienda definisce un piano di formazione e provvede alla relativa attuazione;
- *attività di addestramento*, ovvero attività che in genere sono svolte direttamente "on the job" mediante affiancamento a personale esperto (anche di origine esterna quali consulenti, esperti tecnici, ecc.). I test effettuati periodicamente sui piani di risposta alle emergenze di sicurezza o ambientali rientrano in questa fattispecie.

7.3 CONSAPEVOLEZZA

Le attività di sensibilizzazione sono finalizzate ad informare tutto il personale che opera all'interno del sito dell'Azienda (quindi sia quello dipendente, sia quello di imprese esterne che si trovi ad operare in modo permanente o temporaneo all'interno del sito aziendale) in merito:

- agli aspetti inerenti la SI e i processi aziendali e le attività in cui questi si articolano;
- alla politica per la sicurezza delle informazioni, le procedure, gli obiettivi e i traguardi della Sicurezza delle informazioni, e tutte le altre esigenze applicabili nell'ambito del SGSI adottato dall'Azienda;
- alle possibili ripercussioni negative a livello gestionale/operativo che potrebbero derivare da eventuali comportamenti non conformi in merito a quanto precedentemente specificato;
- alle responsabilità individuali rispetto a quanto enunciato nel punto precedente.

L'Azienda assicura inoltre che il personale delle imprese esterne che si trovi ad operare in modo permanente o temporaneo all'interno del sito aziendale, e il cui lavoro possa provocare un impatto significativo, dimostri di possedere adeguata competenza nello svolgimento degli incarichi attribuitigli e di conoscere le procedure da attivare in caso di incidente o di emergenza.

Le modalità ed i criteri per identificare le necessità, documentare e registrare la formazione sulla SI, individuare le relative responsabilità e competenze vedere il diagramma sotto riportato.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Attività	Funzioni Coinvolte	Documenti
Input: necessità di risorse umane		
Individuazione necessità risorse umane	Direzione - RdF	Richiesta scritta, e-mail o verbale
Definizione delle competenze	RdF - HR	CV Mansionario
Esame richieste da parte della Direzione	Direzione	M9.3 – Riesame della Direzione
Valutazione risorse presenti	RdF - HR	CV Mansionario
Nuove risorse necessarie? (NO / SI)		
Ricerca impiego nuove risorse (selezione)	HR	CV
Addestramento personale per le mansioni necessarie	HR – RGSI - RdF	Piano della formazione Registro formazione interna
Impiego delle risorse umane identificate	Direzione – HR - RGSI	Lettera d'assunzione Zucchetti
Valutazione dell'efficacia dell'addestramento	HR – RGSI	Registro formazione interna
Formazione efficace? (NO / SI)		
Formazione/aggiornamento su SGI, politiche, obiettivi e valutazioni	RGSI – HR	M7.2 – Registro formazione interna
Formazione efficace? (NO / SI)		
Impiego di risorse umane competenti	RdF	
Output: disponibilità di risorse umane		

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

7.4 COMUNICAZIONE

Le comunicazioni rivolte ai collaboratori interni/esterni vengono gestite via mail, in sede di riunioni periodiche e attraverso riunioni dedicate.

RGSI si occupa di coordinare il flusso delle informazioni tra i collaboratori e fornisce all'organizzazione comunicazioni riguardanti l'efficacia del Sistema di gestione per la Sicurezza delle Informazioni.

DOS Group SA ha definito in questa sezione le modalità e tempi per la gestione delle comunicazioni. La registrazione delle comunicazioni viene effettuata tramite apposito modulo "M7.4 – *Registro delle comunicazioni*".

I processi di comunicazione interna possono riguardare la gestione delle comunicazioni di tipo:

- "top-down" (dall'alto al basso);
- "bottom-up" (dal basso all'alto).

Il processo di comunicazione aziendale interna è gestito sulla base di una pianificazione interna dove per ogni evento oggetto di comunicazione viene definito:

- il soggetto responsabile della comunicazione;
- i soggetti destinatari della comunicazione;
- i canali di comunicazione utilizzati (riunioni, comunicati, e-mail, telefono, ecc.).

Processo di gestione della comunicazione interna

SCOPO:	Assicurare al SGSI un corretto ed efficace flusso di informazioni all'interno dell'azienda e ai vari livelli dell'organizzazione		
CAMPO D'APPLICAZIONE	Processo di comunicazione all'interno dell'azienda interno tra i vari livelli funzionali		
RESPONSABILE	**DESCRIZIONE ATTIVITA'**		**DOCUMENTI DI RIFERIMENTO**
RGSI	PIANIFICARE COMUNICAZIONI	Pianifica le attività di comunicazione interna in funzione di vari eventi che necessitano di iniziative a riguardo, incluse le segnalazioni ricevute dal personale interno.	M7.4 Registro delle comunicazioni
RGSI	RILEVARE ISTANZA DI COMUNICAZIONE	Rileva il verificarsi di eventi a fronte dei quali è prevista un'attività di comunicazione interna, incluse le segnalazioni del personale interno che sono registrate in apposito registro	M7.4 Registro delle comunicazioni
RGSI	EFFETTUARE INTERVENTO DI COMUNICAZIONE	Attua le comunicazioni pianificate al verificarsi dell'evento per il quale si rende necessario svolgere un intervento di comunicazione	M7.4 Registro delle comunicazioni
RGSI	RISPONDERE ALLE COMUNICAZIONI	Risponde alle comunicazioni del personale interno registrando le risposte nell'apposito registro	M7.4 Registro delle comunicazioni
RGSI	REGISTRARE INTERVENTI	Registra gli eterventi di comunicazione interna nell'apposito registro	M7.4 Registro delle comunicazioni

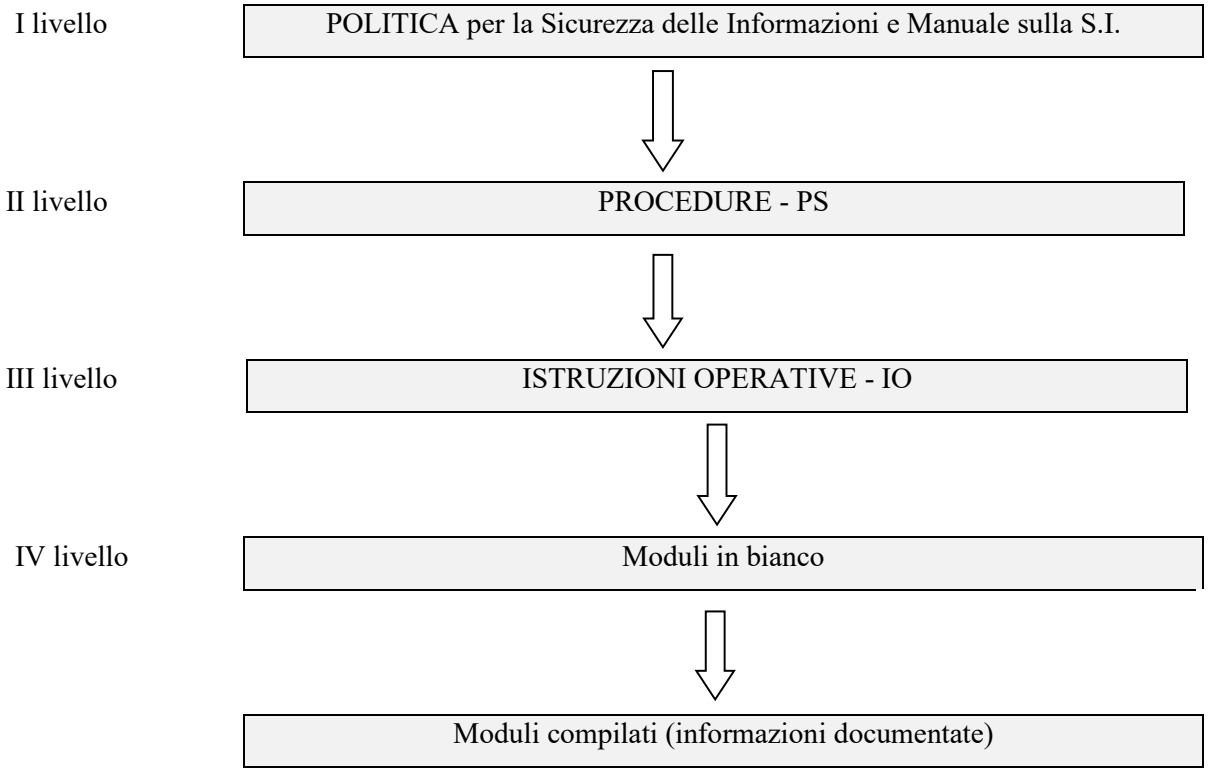
Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

7.5 INFORMAZIONE DOCUMENTATA

7.5.1 Generalità

7.5.2 Creazione e aggiornamento

La documentazione del Sistema di Gestione la Sicurezza delle Informazioni di DOS Group SA è così costituita:



Documenti di I livello: Politica e Manuale della Sicurezza delle Informazioni (MGSI)

Il Manuale della Sicurezza delle Informazioni, sebbene non sia un documento obbligatoriamente richiesto dalla norma, è il documento di base del SGSI che evidenzia la struttura del SGSI e gli indirizzi politici; la struttura organizzativa e le responsabilità. È stato progettato per essere autoportante ed autoesplicativo rispetto alle norme ISO 27001:2017 (copertura di tutti i requisiti). Il manuale rimanda quando necessario a procedure o ad istruzioni per la descrizione dettagliata delle attività. Per la descrizione della Politica si veda oltre.

Documenti di II livello: Procedure (PS)

Sono disposizioni scritte che disciplinano le attività in merito alla Sicurezza delle Informazioni; sono documenti predisposti quando sono coinvolte più funzioni o aree oppure le attività hanno carattere trasversale; sono pensati anche per essere eventualmente inviati all'esterno.

Documenti III livello: Istruzioni Operative (IO)

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Sono disposizioni scritte che specificano o descrivono le modalità operative di esecuzione delle attività. In tali disposizioni vengono indicati anche i metodi, le apparecchiature, i materiali e la sequenza delle operazioni da adottare; sono normalmente pensati per l'utilizzo all'interno dell'organizzazione.

Documenti di IV livello: Moduli in bianco

A questa categoria appartengono i moduli/registri o documenti emessi sui quali verrà registrata l'attività inerente al Sistema di Gestione per la Sicurezza delle Informazioni.

Documenti di registrazione: i Moduli/Registri e ogni alta informazione documentata (documenti di IV livello) possono essere compilati a mano o gestiti in formato elettronico, come meglio specificato nelle procedure ed istruzioni.

Il singolo documento di II e III livello, normalmente, deve essere così strutturato:

- Scopo e campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Modalità
- Chi/come/quando (logica responsabilità)
- Controllo
- Azioni conseguenti
- Registrazioni
- Eventuale riassunto delle Responsabilità
- Eventuale diagramma di flusso riassuntivo
- Altri paragrafi.

I documenti del Sistema di Gestione per la Sicurezza delle Informazioni vengono identificati attraverso un codice alfa numerico ed un titolo.

Nelle procedure, il codice è costituito da PS, che indica che si tratta di una procedura sulla sicurezza delle informazioni e da un numero progressivo:

PS XX

↑ ↑

Procedura

Numero progressivo

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Nelle istruzioni operative, il codice è costituito da IO, che indica che si tratta di una istruzione operativa e da un numero progressivo:

IO YY

Istruzione Operativa

Numero progressivo

Nella modulistica, il codice è costituito da M, che indica che si tratta di un modulo, da un numero progressivo e da due numeri che indicano la Procedura Operativa a cui fa riferimento:

M XX (PS)YY

Modulo

Numero progressivo

Procedura Operativa

Per ogni documento infine viene identificato lo stato di revisione.

7.5.3 Controllo delle informazioni documentate

Tutti i documenti devono seguire il seguente iter di emissione:

- **Redazione** (atto con il quale inizia l'iter di ogni nuovo documento del SGSI)

La Direzione, quando ritiene necessaria la creazione di un nuovo documento del SGSI, incarica chi, a suo parere, risulti più idoneo per elaborare il nuovo documento. La Direzione può decidere se fare visionare tecnicamente il documento ad esperti esterni al fine di verificarne la rispondenza ai requisiti dei documenti di riferimento e la capacità comunicativa richiesta.

- **Verifica** (a cura del responsabile di processo)

Terminata la redazione, il documento viene verificato (riesaminato) e siglato dalla funzione responsabile del processo (in caso di procedure a carattere tecnico) di riferimento al fine di controllarne la coerenza con gli altri documenti del SGSI, con la UNI EN ISO 27001:2017, con l'eventuale Guida applicativa dell'organismo di certificazione e con i documenti di origine esterna (la firma viene apposta solo sui documenti di I, II e III livello). La semplice firma di verifica non autorizza l'emissione del documento.

- **Approvazione** (atto ufficiale che avvalla ogni documento del SGSI)

L'azione è di competenza della Direzione. In questo controllo viene verificata la congruità del documento con la Politica e con gli obiettivi dell'Organizzazione.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

A seguito della firma di approvazione il nuovo documento viene inserito nell'elenco dei documenti del SGSI, eliminando eventuali riferimenti a documenti superati.

Il controllo di tutti i documenti del SGSI è assicurato dunque attraverso apposito modulo "M1PS12 – *Piano documentazione SGSI*" che comprende per ciascun documento:

- descrizione del documento e formato
- identificazione dello stato di revisione corrente
- responsabili dell'emissione e approvazione
- distribuzione
- tempi e luoghi di archiviazione

L'archiviazione degli originali dei documenti del SGSI viene effettuata dal RGSI presso l'archivio di sede nel raccoglitore apposito.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Distribuzione

DOS Group SA provvede a verificare che la documentazione relativa al SGSI sia disponibile ai soggetti aventi diritto.

La modalità di distribuzione dei documenti del SGSI può essere:

- controllata: quando occorre inviare ai destinatari le successive revisioni del documento
- non controllata: quando non occorre inviare ai destinatari le successive revisioni del documento

All'atto di distribuzione di un documento, se in forma controllata, RGSI mantiene evidenza dell'identificazione del documento distribuito e del destinatario. È considerata evidenza oggettiva della distribuzione la firma per ricevuta apposta sulla lettera di trasmissione del documento (se presente) o la ricevuta di una raccomandata, o copia dell'invio e-mail, o infine, verbalizzazione dell'incontro, o attraverso apposito registro.

All'interno di DOS Group SA i documenti vengono distribuiti alle funzioni interessate e coinvolte così come definito nell'elenco dei documenti SGSI e disponibili su server.

La responsabilità degli aggiornamenti, della rimozione delle copie superate e della distribuzione dei documenti del Sistema di Gestione per la Sicurezza delle Informazioni è affidata a RGSI.

La documentazione può essere distribuita, su richiesta, ad eventuali interessati esterni, dietro autorizzazione di RGSI. In questo caso viene espressamente ricordato al ricevente che è sua responsabilità distruggere l'edizione precedente e sostituirla con la revisione inviata (se in forma controllata).

Per la gestione della documentazione, DOS Group SA si attiene ai seguenti principi:

- riservatezza: l'accessibilità ai documenti è possibile solo alle persone espressamente autorizzate;
- reperibilità: i documenti sono reperibili in quanto archiviati secondo procedure stabilite.

Possono accedere alla documentazione solo:

- il personale interno;
- altre persone o enti su espressa autorizzazione di RGSI.

RGSI si assicura che tutte le registrazioni della Sicurezza delle Informazioni siano leggibili e vengano archiviate e conservate in modo da essere prontamente rintracciabili, in luoghi che assicurino condizioni ambientali idonee e per prevenire deterioramenti o danni ed evitare smarrimenti.

Per altre informazioni si rimanda alla "PS12 – *Tenuta sotto controllo dei documenti*" ed alla "PS13 – *Tenuta sotto controllo delle registrazioni*".

Revisione

Ogni revisione deve essere verificata ed approvata dalla stessa funzione che ha rispettivamente verificato e approvato il documento originale.

È facoltà di ogni funzione aziendale segnalare l'opportunità di revisionare un documento mediante comunicazione a RGSI.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

RGSI valuta la richiesta; nel caso la ritenesse motivata, dà inizio al processo di emissione di nuovo documento.

Ogni revisione di un documento comporta dunque lo stesso iter di un documento nuovo (Redazione, Verifica, Approvazione, Registrazione).

Le parti del documento revisionate sono descritte nella tabella in prima pagina.

RGSI si deve assicurare che ogni modifica sia correttamente compresa.

In ogni caso, al fine di facilitare la comprensione ed avere presente in ogni momento lo stato delle revisioni, sulla prima pagina dei documenti di I - II - III livello è stata inserita una maschera che fornisce in dettaglio:

- il numero di revisioni,
- la data in cui queste sono state eseguite,
- il tipo di modifiche apportate,
- il soggetto preposto alla verifica ed approvazione.

Per altre informazioni si rimanda alla "PS12 – *Tenuta sotto controllo dei documenti*" ed alla "PS13 – *Tenuta sotto controllo delle registrazioni*".

Conservazione dei documenti e delle registrazioni

L'archiviazione degli originali dei documenti del SGSI (copia master) viene effettuata da RGSI presso l'archivio di sede nel raccoglitore apposito.

I documenti di registrazione del SGSI compilati (moduli e registri compilati dalle persone indicate nelle procedure che ne prevedono l'applicazione) vengono conservati da RGSI come da indicazioni riportate sul modulo M1PS13. Per quanto riguarda l'eliminazione dei documenti, al termine del periodo previsto, le registrazioni vengono alienate nel rispetto della normativa sulla privacy.

I documenti relativi ad aspetti amministrativi (es. contratti con il cliente) vengono conservati 10 anni, secondo le disposizioni di legge.

Quando previsto contrattualmente, le registrazioni della Sicurezza delle Informazioni sono rese disponibili, per la valutazione, al cliente o ad un suo rappresentante, per un periodo concordato.

Il controllo delle registrazioni riguarda anche le pertinenti registrazioni provenienti dai fornitori.

Conservazione dei documenti del Sistema di Gestione per la Sicurezza delle Informazioni superati

L'originale dei documenti del SGSI superati è conservato da RGSI presso l'archivio unitamente alla versione in vigore e/o nella cartella informatica denominata documenti Superati per almeno 1 anno dalla loro eliminazione o sostituzione con una nuova revisione.

I documenti annullati vengono identificati con il timbro "ANNULLATO" o similare.

Per altre informazioni si rimanda alla "PS12 – *Tenuta sotto controllo dei documenti*" ed alla "PS13 – *Tenuta sotto controllo delle registrazioni*".

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Documenti di origine esterna

È disponibile un elenco dei documenti di origine esterna (per esempio riferimenti a Leggi, Regolamenti, Codici) che hanno diretta e significativa (specificità) influenza sull'attività di DOS Group SA. Diversamente dai documenti del SGSI, non viene tenuta copia dei documenti superati.

Tale modulo riporta le modalità per l'aggiornamento di tali documenti oltre alla collocazione all'interno di DOS Group SA. Se non presente la data, si intende l'ultima edizione pubblicata.

Inoltre tutti i collaboratori interni ed esterni hanno il compito di verificare gli aggiornamenti legislativi utili per lo svolgimento dell'attività, e di farne reciproca segnalazione in qualsiasi momento o durante le riunioni interne.

I documenti di origine esterna non più validi, conservati per qualsiasi motivo, sono identificati attraverso la scritta "annullato" o attraverso forma identificativa equivalente.

Per altre informazioni si rimanda alla "PS12 – *Tenuta sotto controllo dei documenti*" ed alla "PS13 – *Tenuta sotto controllo delle registrazioni*".

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 8

8. ATTIVITÀ OPERATIVE

8.1 PIANIFICAZIONE E CONTROLLI E OPERATIVI

DOS Group SA pianifica e sviluppa i processi richiesti per la realizzazione del servizio/prodotto, coerentemente con i requisiti degli altri processi del sistema di gestione per la sicurezza delle informazioni e necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto azioni per affrontare eventuali rischio o cogliere delle opportunità:

Vengono quindi definiti, quando appropriati:

- Piani per conseguire obbiettivi per la sicurezza
- criteri per il controllo dei processi e per l'accettazione;
- le risorse necessarie per ottenere la conformità del servizio/prodotto;
- le informazioni documentate necessarie ad assicurare la conformità del servizio/prodotto.
- Documentazione di riferimento incluse le registrazioni.

La conservazione di tali registrazioni è descritta nel presente MGSI e in apposita procedura documentata "PS13 - *Tenuta sotto controllo delle registrazioni*".

Outsourcing

DOS Group SA non si avvale di società esterne per l'erogazione dei propri servizi.

8.2 VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

L'organizzazione ha stabilito e valutato il rischio relativo alla SI conservando le informazioni documentate sui risultati delle valutazioni vedi:

PS04B - Piano per la valutazione dei rischi per la sicurezza delle informazioni

8.3 TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

La DOS Group SA ha attuato il piano per il trattamento del rischio conservando le informazioni documentate sui risultati del trattamento posto in campo a supporto della Sicurezza delle informazioni vedi:

PS06 - Piano per il trattamento del rischio

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 9

9. VALUTAZIONE DELLE PRESTAZIONI

9.1 MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE

Generalità

DOS Group SA pianifica e attua i processi di monitoraggio, di misurazione, di valutazione, analisi e di miglioramento necessari a:

- dimostrare la conformità dei servizi erogati ai requisiti specificati nella Sicurezza delle informazioni;
- assicurare la conformità del sistema di gestione per la Sicurezza delle informazioni;
- migliorare in modo continuo l'efficacia del sistema di gestione per la Sicurezza delle Informazioni.

A tale scopo, si rimanda al documento "M6.2 – *Piano di miglioramento SI*" dove, per ciascun processo, sono stati definiti precisi indicatori di monitoraggio e pertinenti criteri, modalità e tempi di valutazione e analisi.

Un'analisi complessiva e critica di risultati e performances, viene elaborata in sede di riesame della Direzione.

L'organizzazione pianifica ed attua i processi di misurazione, analisi e miglioramento necessari a:

a) assicurare la conformità del SGSI attraverso l'analisi dei processi e relativo monitoraggio;

b) migliorare in modo continuo l'efficacia del SGSI attraverso il monitoraggio del piano degli obiettivi e attraverso il riesame della Direzione.

I metodi utilizzati possono includere tecniche statistiche (calcoli, diagrammi ed istogrammi, ecc.) da riportare nei rapporti di RGSI alla Direzione.

L'utilizzo di tecniche di rilevamento, analisi e valutazione dei dati di natura statistica è estremamente importante per una corretta e consapevole garanzia della prestazione e dei servizi nel tempo. Le informazioni delle statistiche devono essere tempestive ed utilizzate anche nelle decisioni operative.

Sono considerate necessità strategiche per il continuo miglioramento le rilevazioni relative a:

- analisi delle non conformità;
- analisi dei reclami;
- analisi degli incident;
- analisi delle azioni correttive e azioni di miglioramento;
- dati sui fornitori.

Tali valutazioni devono essere utilizzati per:

a. dimostrare conformità del servizio/prodotto ai requisiti
b. assicurare conformità ed efficacia del SGSI
c. dimostrare che la pianificazione è stata attuata con successo

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

d. valutare le prestazioni dei processi e dei fornitori esterni
e. determinare le esigenze e le opportunità di miglioramento nell'ambito del SGSI
f. determinare idoneità, l'adeguatezza e l'efficacia del SGSI

Le suddette rilevazioni sono effettuate in modo sistematico, sotto la responsabilità della Direzione. I risultati sono presentati alla Direzione in fase di Riesame del Sistema. Durante tali riunioni sono inoltre decise eventuali altre necessità statistiche che devono essere indagate e le relative modalità di esecuzione; nelle riunioni successive sarà controllata l'applicazione di quanto deciso.
L'organizzazione ha individuato i dati appropriati per dimostrare l'adeguatezza ed efficacia del SGSI e per valutare dove possono essere apportati miglioramenti continui dell'efficacia del SGSI. L'analisi dei dati viene raccolta nei rapporti alla Direzione a cura di RGSI, quale input al riesame della Direzione (rif. par. 9.3 del MGSI).
La raccolta dei dati, elaborata con l'ausilio di eventuali tecniche statistiche riporta solitamente informazioni e risultati relativi a:

- conformità ai requisiti della SI;
- caratteristiche e andamento dei processi;
- andamento dei fornitori/forniture.

L'organizzazione ha adottato adeguati metodi per monitorare e, ove applicabile, misurare i processi del SGSI identificati nel presente MGSI, al fine di dimostrare la capacità dei processi di ottenere i risultati pianificati.
A tale scopo sono definiti, nel piano di miglioramento (rif. mod. M6.2), obiettivi pianificati e misurabili per i processi individuati, comprendenti:

a) identificazione del processo;
b) obiettivo per quel processo;
c) indicatore di misura attuale (numerico o percentuale);
d) indicatore di misura che si vuol raggiungere (numerico o percentuale);
e) identificazione delle eventuali risorse/investimenti per quell'obiettivo;
f) pertinente livello/funzione dell'organizzazione responsabile del raggiungimento dell'obiettivo;
g) metodologia di misurazione (ogni quanto e come) per il raggiungimento dell'obiettivo.

Periodicamente (almeno ogni sei mesi) sono monitorati i processi al fine di rispettare quanto pianificato. Qualora i risultati non siano raggiunti, sono adottate opportune azioni correttive per assicurarne il raggiungimento.
Per quanto riguarda, invece, il monitoraggio dei processi produttivi essi sono stati identificati con opportuni diagrammi di flusso

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

9.2 AUDIT INTERNO

Al fine di accertare la corretta applicazione, il funzionamento e l'efficacia del SGSI e per verificare se i risultati siano in linea con quanto atteso e con la Politica per la Sicurezza delle Informazioni sono pianificati e attuati gli audit interni.

La pianificazione viene predisposta da RGSI su apposito modulo "M1PSXX – *Programma di audit interno*" e prevede che almeno una volta l'anno siano verificate tutte le aree aziendali e tutti i punti del Sistema di Gestione per la Sicurezza delle Informazioni; la Direzione è responsabile della corretta applicazione del programma.

La programmazione viene effettuata in base all'importanza che l'area o il processo da verificare hanno sulla sicurezza delle informazioni: nella pianificazione sono individuati i responsabili delle verifiche garantendo la competenza del verificatore e la sua imparzialità.

I risultati delle verifiche sono registrati su apposito rapporto (rif. M3PS15) e portati a conoscenza dei responsabili delle aree verificate. I responsabili delle aree verificate intraprendono tempestive azioni correttive relativamente alle carenze evidenziate. Tale attività viene gestita sul modulo "M1PS15 – *Rapporto di NC e AC*".

Gli audit interni hanno anche la funzione di controllare l'applicazione delle misure correttive prese a fronte di rilievi di visite precedenti ed appurare l'efficacia di tali azioni.

I resoconti degli audit interni sono analizzati dalla Direzione durante le riunioni di Riesame del Sistema.

Gli audit interni sono eseguiti eventualmente con l'utilizzo di liste di riscontro, al fine di garantire la sistematicità delle valutazioni, oppure seguendo le istruzioni di processo. Le osservazioni sono registrate sulle liste di riscontro stesse.

La Direzione può decidere ulteriori visite in funzione di particolari esigenze.

Spetta a RGSI scegliere la persona che dovrà eseguire l'audit (auditor); questa persona, interna od esterna all'azienda, deve aver frequentato con successo un corso per valutatore interno e deve avere almeno due anni di esperienza nel campo dei sistemi sulla sicurezza delle informazioni.

Il RGSI inoltre può optare per una composizione del gruppo più ampia, all'interno di esse viene comunque sempre scelto un responsabile di verifica.

L'auditor deve sforzarsi sempre di essere imparziale, dando il giusto peso alle opinioni ed alle osservazioni degli interlocutori e svolgendo nello stesso tempo con massima fermezza ed obiettività la propria attività ispettiva. Deve inoltre operare con la massima attenzione e correttezza.

Nota: sono considerati adeguati i corsi i cui contenuti sono equivalenti a quelli approvati da organismi di certificazione del personale (auditor) accreditati.

L'organizzazione effettua, ad intervalli predefiniti, audit interni al fine di stabilire la conformità del SGSI secondo quanto pianificato. Questo con particolare riferimento anche ai processi aventi rilevanza strategica.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Gli obiettivi degli audit interni del SGSI sono finalizzati a verificare se il SGSI:

- è conforme a quanto pianificato, ai requisiti delle norme internazionale ed ai requisiti del SGSI stabiliti dall'organizzazione stessa;
- è stato efficacemente attuato e mantenuto aggiornato;

fornendo quindi alla Direzione i necessari ritorni in merito.

La programmazione e la pianificazione degli audit interni sono attuate facendo riferimento alla norma UNI EN ISO 19011:2018 "Linee guida per audit di sistemi di gestione", così come definito in apposita procedura documentata "PS14 - *Audit interno*".

Gli audit interni possono essere svolti sia da personale aziendale interno sia da personale esterno (auditor ed esperti tecnici) opportunamente qualificato al fine di assicurare indipendenza ed imparzialità allo stesso processo di audit.

I risultati degli audit interni del SGSI, documentati attraverso i rapporti di audit interno, concorrono al riesame di Direzione (rif. par. 9.3 del MGQSI).

9.3 RIESAME DI DIREZIONE

Annualmente DOS Group SA effettua un riesame periodico del Sistema di Gestione per la Sicurezza delle Informazioni. Tale attività avviene in forma di riunione alla quale devono essere presenti RGSI e le funzioni pertinenti. In tali riunioni possono essere coinvolti altri soggetti su richiesta di uno dei membri ed autorizzazione della Direzione.

Con cadenza annuale devono essere discussi e presi in considerazione, durante una o più riunioni, almeno tutti i punti seguenti:

a. Verifica azioni decise nelle precedenti riunioni in merito alla sicurezza delle informazioni;
b. Cambiamenti del contesto e della strategia
c. Informazioni sulle prestazioni del SGSI che comprendono
    - Non conformità e azioni correttive
    - Risultati di monitoraggi e misurazioni
    - Risultati degli audit
    - Questioni riguardanti i fornitori esterni e le altre parti interessate
    - Adeguatezza risorse necessarie
    - Performances di processo
d. Efficacia delle azioni intraprese per affrontare rischi e opportunità
e. Nuove potenziali opportunità per miglioramento continuo

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Tali riunioni sono documentate con rapporti, predisposti da RGSI, che è il responsabile del riesame; i rapporti sono portati a conoscenza degli interessati (Responsabili di area e soggetti coinvolti nelle azioni decise) e archiviati a cura di RGSI.

Per tale attività si utilizza per la registrazione il modulo "M9.3 – *Verbale di riesame della direzione*".

I risultati del riesame devono comprendere decisioni ed azioni relative:

a. al miglioramento dell'efficacia del Sistema di gestione per la sicurezza delle informazioni ed i loro processi, comprese le risorse necessarie;
b. opportunità di miglioramento;
c. piano di addestramento del personale.

Processo di gestione del Riesame della Direzione

SCOPO:	Guidare la fase di riesame delle direzione ed indicare la modalità di convocazione conduzione, di verbalizzazione e di registrazione. Si tende in tal modo a favorire il lavoro della Direzione, indicando i temi fondamentali da considerare durante le fasi di esame. A questi temi vanno aggiunti quelli che la Direzione riterrà di volta in volta influenti sulla qualità del SGSI		
CAMPO D'APPLICAZIONE	Applicata in sede di Riesame della Direzione		
RESPONSABILE	**DESCRIZIONE ATTIVITA'**		**DOCUMENTI DI RIFERIMENTO**
DIR	PIANIFICARE RIESAME	Pianifica lo svolgimento del riesame sia in funzione di programmazione annua sia in funzione di eventi straordinari (NC, incident etc)	
RGSI	PROGRAMMARE RIESAME	Programmare il riesame della Direzione in funzione dei dati e dei documenti da raccogliere	
FUNZIONI AZIENDALI	PREDISPORRE DATI E DOCUMENTI	Predispongono per la parte di competenza i dati ed i documenti richiesti	Documenti vari
RGSI	PREPARARE RIESAME	Prepara i dati ed i documenti mediante opportuna elaborazione, riferendoli per quanto possibile ai processi aziendali e alle relative prestazioni	Documenti vari
DIR	SVOLGERE RIESAME	Effettua il riesame del SGSI prendendo le opportune decisioni per il miglioramento del SGSI nonché dei processi/prestazioni aziendali	
RGSI	REDIGE VERBALE DI RIESAME PREDISPONE IL PIANO DI MIGLIORAMENTO	Redige verbale della riunione di Riesame e predispone la bozza del piano di miglioramento strutturato per processi e prestazioni	M 9.3 Verbale di Riesame della Direzione
DIR	VERIFICARE ED APPROVARE IL PIANO DI MIGLIORAMENTO	Verificare ed approvare il piano di miglioramento previa eventuale correzione/integrazione dello stesso, la dove si necessità identificare la copertura finanziaria necessaria	M 6.2 Piano di miglioramento
DIR	COMUNICARE IL PIANO DI MIGLIORAMENTO	Comunicare il Piano di Miglioramento alle funzioni aziendali di competenza definendo attività, tempistiche e responsabilità di svolgimento delle relative azioni	M 6.2 Piano di miglioramento
RGSI	MONITORARE IL PIANO DI MIGLIORAMENTO	Monitorare l'attuazione del piano di miglioramento e segnalare alla Direzione eventuali necessità di modifiche o integrazioni	M 6.2 Piano di miglioramento
DIR	VERIFICARE/APPROVARE IL PIANO DI MIGLIORAMENTO	Verifcare/approvare eventuali aggiornamenti al piano di miglioramento	M 6.2 Piano di miglioramento

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

SEZIONE 10

10. MIGLIORAMENTO

10.1 GENERALITÀ

Il miglioramento continuo dei servizi offerti ai clienti e del suo SGSI è uno degli obiettivi primari di DOS Group SA.

L'organizzazione si impegna a migliorare con continuità l'efficacia del suo SGSI, utilizzando la politica per la sicurezza delle informazioni, gli obiettivi, i risultati degli audit, l'analisi dei dati, le AC ed i riesami della Direzione.

L'organizzazione crede fermamente nel miglioramento continuo del proprio SGSI. Per far ciò utilizza:

- la politica per la sicurezza delle informazioni;
- gli obiettivi per la sicurezza delle informazioni;
- i risultati degli audit;
- l'analisi dei dati;
- le azioni correttive;
- i riesami da parte della Direzione.

10.2 NON CONFORMITÀ ED AZIONI CORRETTIVE

L'obiettivo del continuo miglioramento è raggiungibile anche attraverso una corretta ed efficace gestione delle AC.

La gestione delle suddette azioni è effettuata attraverso un processo che permetta una completa gestione dell'attività.

Le azioni intraprese devono essere in relazione all'influenza della non conformità sulla sulla sicurezza delle informazioni e del rischio connesso.

La pianificazione del processo di gestione è stata effettuata con la predisposizione del modulo "M1PS15 – *Rapporto di NC e AC*", che è un piano dettagliato di intervento, in cui devono essere indicati:

- l'analisi delle cause
- le azioni decise con relative responsabilità e tempi
- descrizione delle azioni necessarie
- la verifica di attuazione ed efficacia dell'azione intrapresa

Al rapporto di NC sono allegati se necessario tutti i documenti di dettaglio utili alla comprensione del lavoro.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

I moduli sono identificati in modo numerico progressivo per anno e archiviati in raccoglitore specifico.

Azioni correttive

Le AC sono intese ad eliminare le cause di una non conformità e devono essere appropriate agli effetti delle NC riscontrate.

L'analisi dei rapporti di non conformità è svolta almeno una volta all'anno, durante il Riesame del Sistema. Dall'esame di questa documentazione la Direzione, supportato dal RGSI ed il personale interessato, individua i problemi prioritari ed elabora una strategia per la loro soluzione, indicando i tempi e le responsabilità.

I risultati di questa analisi vengono registrati dal RGSI nel modulo "M1PS15 – *Rapporto di NC e AC*" nel quale vengono inoltre specificati il tipo di AC che si è deciso di intraprendere e successivamente le verifiche attuate per controllarne l'attuazione e l'efficacia.

Si noti che si può dar corso ad una AC:

- a seguito di precisa richiesta di clienti che abbiano riscontrato problemi in merito alla SI del servizio/prodotto fornito o alla sicurezza delle informazioni;
- per decisione interna, a seguito di riesami intesi a valutare lo stato di applicazione del sistema o di sue parti.

In occasione del riesame periodico dei rapporti di NC, la Direzione prende in esame con attenzione particolare anche le contestazioni e segnalazioni dei clienti, i risultati delle Verifiche ispettive interne ed esterne e le registrazioni della sicurezza delle informazioni, allo scopo di individuare i problemi ricorrenti o di particolare gravità. Verifica dunque con le funzioni interessate che siano note le cause prime e la possibilità di effettuare interventi atti a rimuoverle. Assegna di conseguenza le priorità, privilegiando le AC richieste da clienti o provocate da reclami. Gli interessati pianificano e portano a termine le necessarie AC.

Nel caso specifico delle anomalie di SGSI, le AC possono consistere in:

- modifica di procedure e/o di pratiche operative;
- stesura di nuovi documenti (ad es. a carattere esplicativo o addestrativo);
- addestramento o riaddestramento del personale.

DOS Group SA mantiene registrazione di tali rapporti di NC in apposito raccoglitore per le opportune analisi e valutazioni.

L'organizzazione intraprende azioni volte ad eliminare le cause delle non conformità, al fine di prevenirne la ripetizione. Le azioni correttive sono appropriate agli effetti delle non conformità riscontrate.

È predisposta una procedura documentata "PS15 - *Gestione delle NC e AC*" ove sono specificati i requisiti per:

a) riesaminare le non conformità (compresi i reclami dei clienti);
b) individuare le cause delle non conformità;
c) valutare l'esigenza di azioni per assicurare che le non conformità si ripetano;

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

d) determinare ed effettuare le azioni necessarie;

e) registrare i risultati delle azioni effettuate;

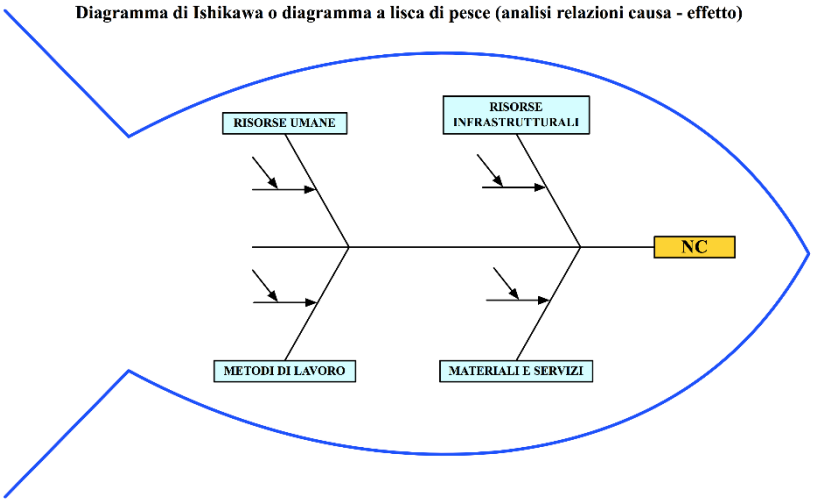
f) esaminare l'efficacia delle azioni correttive effettuate.

In particolare l'analisi delle cause delle NC è svolta adottando la metodologia di Ishikawa (o analisi di relazione causa-effetto "a lisca di pesce"). Tale metodologia individua le cause di qualsivoglia situazione non conforme facendo riferimento ad una o più delle seguenti tipologie di causa:

- cause relative a risorse infrastrutturali;
- cause relative a risorse umane;
- cause relative a beni o servizi utilizzati;
- cause relative a metodi di lavoro.

Per ognuna delle cause primarie sopra individuate è possibile individuare vari livelli di sottocausa come da diagramma sotto rappresentato.

Diagramma di Ishikawa o diagramma a lisca di pesce (analisi relazioni causa - effetto)



10.3 MIGLIORAMENTO CONTINUO

La sicurezza delle informazioni è un obiettivo primario per DOS Group SA e può essere raggiunto solo con l'impegno ed il contributo di tutti.

Ai clienti devono essere offerti i servizi che desiderano e che considerano essere in linea con i risultati attesi della Sicurezza delle informazioni, cercando sempre di superare le loro aspettative. Tale obiettivo deve essere raggiunto coinvolgendo il cliente in un'ottica di partecipazione; bisogna portare il cliente nell'impresa e nel servizio/prodotto al fine di renderlo consapevole e coinvolgerlo nella definizione della prestazione.

Soddisfare il cliente è uno degli impegni più difficili, soprattutto considerando che deve essere fatto in modo efficiente e redditizio, per cui servono miglioramento continuo ed innovazione. A tal fine, l'organizzazione si impegna in una costante ricerca del miglioramento dell'idoneità, adeguatezza ed efficacia del SGSI attraverso un'adeguata investigazione sulle performances.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.

Tutti i collaboratori di DOS Group SA indipendentemente dalle responsabilità e dal ruolo, devono lavorare affinché il lavoro sia sinergico e ognuno possa portare il proprio contributo.

Il presente documento è di proprietà di DOS GROUP SA e non può essere riprodotto o comunicato a terzi senza autorizzazione scritta.