SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Manuale SGSI

NetJoin Srl è una società specializzata nella progettazione, realizzazione e gestione di infrastrutture digitali e servizi ICT avanzati per aziende, operatori e pubbliche amministrazioni.
L'azienda opera nei settori delle telecomunicazioni, del networking, del cloud computing e della cybersecurity, offrendo soluzioni integrate per connettività Internet, reti dati, infrastrutture in fibra ottica, sistemi wireless, servizi IP, datacenter, hosting, housing, colocation e servizi cloud pubblici, privati e ibridi.
NetJoin Srl fornisce inoltre servizi di system integration, consulenza informatica, progettazione e gestione di infrastrutture IT, virtualizzazione, business continuity, disaster recovery, monitoraggio e gestione di reti e sistemi, nonché attività di supporto tecnico specialistico e manutenzione evolutiva.
La società sviluppa e gestisce infrastrutture di comunicazione elettronica e piattaforme digitali ad alta affidabilità, con particolare attenzione alla sicurezza delle informazioni, alla resilienza dei servizi, alla continuità operativa e all'innovazione tecnologica.
NetJoin Srl opera secondo principi di qualità, affidabilità e miglioramento continuo, adottando processi organizzativi e tecnici finalizzati alla protezione delle informazioni, alla soddisfazione del cliente e alla conformità normativa applicabile.

Codice	SGSI-MAN-001
Data documento	15/05/2026
Versione	00
Approvato da	Alta direzione

PRESENTAZIONE

Il presente documento è redatto per fornire una rappresentazione organica, elegante e professionale del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione, collegando business, asset, rischi, controlli, responsabilità e miglioramento continuo in un impianto coerente con la ISO/IEC 27001:2022.

SCOPO

Lo scopo del documento è supportare direzione, funzioni aziendali, auditor, consulenti e parti autorizzate nella comprensione del perimetro del SGSI, della logica di governo adottata, delle priorità di rischio e delle misure poste a presidio delle informazioni e dei servizi rilevanti.

DESCRIZIONE DELL'AZIENDA

NetJoin Srl è una società specializzata nella progettazione, realizzazione e gestione di infrastrutture digitali e servizi ICT avanzati per aziende, operatori e pubbliche amministrazioni.
L'azienda opera nei settori delle telecomunicazioni, del networking, del cloud computing e della cybersecurity, offrendo soluzioni integrate per connettività Internet, reti dati, infrastrutture in fibra ottica, sistemi wireless, servizi IP, datacenter, hosting, housing, colocation e servizi cloud pubblici, privati e ibridi.
NetJoin Srl fornisce inoltre servizi di system integration, consulenza informatica, progettazione e gestione di infrastrutture IT, virtualizzazione, business continuity, disaster recovery, monitoraggio e gestione di reti e sistemi, nonché attività di supporto tecnico specialistico e manutenzione evolutiva.
La società sviluppa e gestisce infrastrutture di comunicazione elettronica e piattaforme digitali ad alta affidabilità, con particolare attenzione alla sicurezza delle informazioni, alla resilienza dei servizi, alla continuità operativa e all'innovazione tecnologica.
NetJoin Srl opera secondo principi di qualità, affidabilità e miglioramento continuo, adottando processi organizzativi e tecnici finalizzati alla protezione delle informazioni, alla soddisfazione del cliente e alla conformità normativa applicabile.

DESCRIZIONE DEL SERVIZIO

NetJoin Srl fornisce servizi professionali e soluzioni avanzate nei settori ICT, cybersecurity, telecomunicazioni, networking e cloud computing, con particolare specializzazione nella protezione delle infrastrutture digitali critiche, nella sicurezza delle reti e nella continuità operativa dei servizi.
La società progetta, realizza e gestisce infrastrutture di rete ad alta affidabilità, servizi di comunicazione elettronica e piattaforme cloud, adottando tecnologie e procedure orientate alla resilienza, alla sicurezza delle informazioni e alla mitigazione delle minacce informatiche.
I principali servizi offerti comprendono:
progettazione, implementazione e gestione di infrastrutture di rete IP, reti dati, backbone in fibra ottica, sistemi wireless e piattaforme di comunicazione elettronica;
servizi Internet, connettività dedicata, transito IP, peering, interconnessione e gestione di infrastrutture ISP;
progettazione e gestione di infrastrutture cloud pubbliche, private e ibride, ambienti virtualizzati, hosting, housing, colocation e servizi datacenter;
servizi avanzati di cybersecurity, protezione perimetrale, segmentazione di rete, hardening infrastrutturale, controllo accessi e monitoraggio continuo della sicurezza;
progettazione e gestione di sistemi di protezione anti-DDoS e mitigazione del traffico malevolo, finalizzati alla protezione di servizi Internet, infrastrutture critiche e piattaforme digitali;
monitoraggio proattivo delle reti e dei sistemi, analisi degli eventi di sicurezza, gestione incidenti e supporto alle attività di risposta e remediation;
implementazione di soluzioni per business continuity, disaster recovery, alta affidabilità e resilienza infrastrutturale;
attività di system integration, migrazione infrastrutturale, consolidamento e ottimizzazione di sistemi hardware e software;
consulenza specialistica in ambito cybersecurity, telecomunicazioni, networking, infrastrutture cloud e trasformazione digitale;
assistenza tecnica specialistica, supporto sistemistico e manutenzione correttiva ed evolutiva di infrastrutture IT;
progettazione e manutenzione di impianti tecnologici, elettrici e trasmissione dati correlati alle infrastrutture ICT;
noleggio operativo, gestione e fornitura di apparati hardware, dispositivi di sicurezza, apparati di rete e piattaforme tecnologiche integrate;
servizi professionali di formazione tecnica, affiancamento specialistico e supporto operativo qualificato.
NetJoin Srl opera secondo principi di sicurezza, affidabilità, riservatezza, disponibilità e miglioramento continuo, adottando processi organizzativi e tecnici finalizzati alla protezione delle informazioni, alla continuità dei servizi e alla conformità normativa applicabile.

INDICE DEL DOCUMENTO

TERMINI IN USO

Termine	Definizione
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni.
Informazione	Dato o insieme di dati rilevanti per l'organizzazione, indipendentemente dal formato o supporto.
Asset	Qualsiasi risorsa informativa, organizzativa, tecnologica, fisica o di supporto rilevante per il SGSI.
Rischio	Effetto dell'incertezza sugli obiettivi, valutato in termini di probabilità e impatto.
Controllo	Misura organizzativa, fisica o tecnica adottata per modificare o presidiare il rischio.
Trattamento del rischio	Decisione e insieme di azioni per mitigare, trasferire, evitare o accettare un rischio.
SoA	Statement of Applicability: documento che riporta i controlli applicabili, il relativo stato e la giustificazione.
Parte interessata	Soggetto interno o esterno che può influenzare, essere influenzato o percepirsi influenzato dal SGSI.

1. SCOPO E FINALITÀ DEL MANUALE

1.1 Scopo del manuale

Il presente Manuale SGSI definisce l’architettura di governo, i criteri metodologici, i ruoli, i processi e le regole operative mediante cui NetJoin S.r.l. istituisce, attua, mantiene e migliora il proprio Sistema di

Gestione per la Sicurezza delle Informazioni. Il manuale costituisce il riferimento di alto livello del sistema e raccorda contesto organizzativo, analisi dei rischi, piano di trattamento, controlli applicabili, procedure operative, riesame e miglioramento continuo, in coerenza con i requisiti della ISO/IEC 27001 e con le migliori pratiche internazionali di governance.

1.2 Profilo aziendale

NetJoin Srl è una società specializzata nella progettazione, realizzazione e gestione di infrastrutture digitali e servizi ICT avanzati per aziende, operatori e pubbliche amministrazioni.
L'azienda opera nei settori delle telecomunicazioni, del networking, del cloud computing e della cybersecurity, offrendo soluzioni integrate per connettività Internet, reti dati, infrastrutture in fibra ottica, sistemi wireless, servizi IP, datacenter, hosting, housing, colocation e servizi cloud pubblici, privati e ibridi.
NetJoin Srl fornisce inoltre servizi di system integration, consulenza informatica, progettazione e gestione di infrastrutture IT, virtualizzazione, business continuity, disaster recovery, monitoraggio e gestione di reti e sistemi, nonché attività di supporto tecnico specialistico e manutenzione evolutiva.
La società sviluppa e gestisce infrastrutture di comunicazione elettronica e piattaforme digitali ad alta affidabilità, con particolare attenzione alla sicurezza delle informazioni, alla resilienza dei servizi, alla continuità operativa e all'innovazione tecnologica.
NetJoin Srl opera secondo principi di qualità, affidabilità e miglioramento continuo, adottando processi organizzativi e tecnici finalizzati alla protezione delle informazioni, alla soddisfazione del cliente e alla conformità normativa applicabile.

1.3 Campo di applicazione di alto livello

Il SGSI è concepito per proteggere informazioni, asset, processi e servizi che sostengono gli obiettivi aziendali, salvaguardando riservatezza, integrità, disponibilità, autenticità e tracciabilità dove necessario.

1.4 Politica per la sicurezza delle informazioni

La Direzione si impegna a garantire che la sicurezza delle informazioni sia allineata agli obiettivi di business, sostenuta da adeguate risorse, integrata nei processi aziendali e riesaminata periodicamente per assicurarne efficacia, pertinenza e miglioramento continuo.

2. CAMPO DI APPLICAZIONE DEL SGSI

Il Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni di NetJoin Srl si applica alle attività di progettazione, realizzazione, gestione, monitoraggio e manutenzione di infrastrutture ICT, reti dati, servizi di telecomunicazione, servizi Internet, piattaforme cloud e servizi di cybersecurity.
Lo scopo comprende l'erogazione di servizi di connettività IP, transito, peering, hosting, housing, colocation, virtualizzazione, monitoraggio infrastrutturale, protezione anti-DDoS, gestione della sicurezza delle reti, business continuity, disaster recovery, assistenza tecnica specialistica, system integration e consulenza ICT.
Sono inclusi nel perimetro SGSI i sistemi informativi aziendali, le infrastrutture di rete, i sistemi cloud e virtualizzati, gli apparati di sicurezza, le piattaforme di monitoraggio, i sistemi documentali e le informazioni trattate nell'ambito dell'erogazione dei servizi ai clienti.
Il sistema si applica presso la sede operativa e alle attività svolte da personale interno e collaboratori autorizzati, secondo ruoli e responsabilità definiti dall'organizzazione.

Il perimetro del SGSI comprende persone, processi, informazioni, tecnologie, servizi e siti inclusi nell'ambito dichiarato, nonché gli asset e i trattamenti correlati che possono influire su riservatezza, integrità e disponibilità delle informazioni rilevanti per l'organizzazione e per le parti interessate.

2.1 Confini fisici, logici e organizzativi

I confini del sistema includono le sedi, le unità organizzative, le piattaforme, le infrastrutture, i servizi e i flussi informativi ricompresi nel perimetro dichiarato. Sono inclusi anche i fornitori critici, i processi esternalizzati e gli ambienti digitali che trattano o supportano informazioni rilevanti per il business.

3. RIFERIMENTI NORMATIVI E CRITERI DI CONFORMITÀ

3.1 Riferimenti applicabili

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR / Regolamento (UE) 2016/679
- NIS2 ove applicabile
- Obblighi contrattuali e requisiti cliente
- Policy, procedure e registrazioni interne del SGSI

3.2 Criteri di conformità

Il sistema è sviluppato assumendo come quadro di riferimento la ISO/IEC 27001, la Statement of Applicability aziendale, le procedure interne, gli obblighi contrattuali, i requisiti cogenti applicabili e gli impegni assunti verso clienti, partner, personale, fornitori e altre parti interessate. Eventuali requisiti aggiuntivi di natura legale, regolatoria, settoriale o contrattuale devono essere recepiti nei registri, nei controlli e nei piani di azione del SGSI.

4. CONTESTO DELL'ORGANIZZAZIONE E PARTI INTERESSATE

4.1 Analisi del contesto interno

NetJoin Srl è una società operante nel settore ICT e telecomunicazioni specializzata nella gestione di infrastrutture digitali, networking, cybersecurity e servizi cloud. L'organizzazione è strutturata con una gestione centralizzata dei processi tecnici, operativi e amministrativi.
Le attività aziendali dipendono dalla disponibilità e affidabilità delle infrastrutture IT, dei sistemi di rete, dei sistemi di monitoraggio e delle piattaforme cloud utilizzate per l'erogazione dei servizi ai clienti.
I principali fattori interni rilevanti per il SGSI comprendono:
protezione delle informazioni aziendali e dei dati dei clienti;
continuità operativa dei servizi erogati;
resilienza delle infrastrutture di rete e sicurezza perimetrale;
gestione degli accessi privilegiati e degli account amministrativi;
monitoraggio e mitigazione di minacce informatiche e attacchi DDoS;
competenze tecniche specialistiche del personale e dei collaboratori;
gestione documentale, backup e disaster recovery;
dipendenza da infrastrutture cloud, datacenter e connettività Internet.
L'organizzazione adotta procedure operative, controlli tecnici e misure di sicurezza finalizzate a garantire riservatezza, integrità, disponibilità e tracciabilità delle informazioni.

4.2 Analisi del contesto esterno

NetJoin Srl opera in un mercato caratterizzato da elevata evoluzione tecnologica, crescente esposizione alle minacce cyber e forte dipendenza dalla continuità dei servizi digitali.
I principali fattori esterni rilevanti comprendono:
evoluzione continua delle minacce informatiche, incluse campagne DDoS, ransomware, compromissioni di rete e vulnerabilità software;
requisiti normativi e contrattuali relativi a protezione dei dati, sicurezza delle informazioni e continuità operativa;
dipendenza da fornitori di connettività, datacenter, cloud provider e vendor tecnologici;
esigenze dei clienti in termini di affidabilità, disponibilità, sicurezza e tempi di risposta;
rischi derivanti da interruzioni di servizio, incidenti cyber e indisponibilità infrastrutturali;
necessità di aggiornamento continuo delle competenze tecniche e delle tecnologie adottate;
requisiti di conformità relativi a ISO 9001, ISO/IEC 27001 e normative applicabili in ambito ICT e telecomunicazioni.
L'organizzazione monitora costantemente il contesto tecnologico e normativo al fine di adeguare processi, controlli e misure di sicurezza.

4.3 Parti interessate e relative esigenze

Le principali parti interessate rilevanti per il Sistema di Gestione Integrato sono:
Clienti: richiedono continuità dei servizi, protezione delle informazioni, affidabilità infrastrutturale, riservatezza e tempi di risposta adeguati;
Fornitori e partner tecnologici: richiedono collaborazione operativa, conformità tecnica e gestione coordinata delle attività;
Collaboratori e personale autorizzato: richiedono procedure chiare, strumenti adeguati, formazione e sicurezza operativa;
Autorità e organismi normativi: richiedono conformità alle normative applicabili e corretta gestione delle informazioni;
Cloud provider, carrier e datacenter partner: richiedono rispetto dei requisiti contrattuali, tecnici e di sicurezza;
Organismo di certificazione: richiede mantenimento dell'efficacia del sistema di gestione e miglioramento

continuo;
Proprietà e direzione aziendale: richiedono controllo dei rischi, continuità operativa, qualità dei servizi e tutela del patrimonio informativo.

L’organizzazione valuta periodicamente le evoluzioni del contesto e le aspettative delle parti interessate, verificandone l’impatto sul perimetro, sui rischi, sui controlli e sulla documentazione del sistema.

5. LEADERSHIP, GOVERNO E RESPONSABILITÀ

5.1 Ruoli, responsabilità e autorità

La Direzione assicura indirizzo strategico, disponibilità delle risorse, integrazione del SGSI nei processi aziendali, approvazione delle politiche e riesame periodico delle prestazioni del sistema. I responsabili di funzione e gli owner degli asset presidiano i rischi di competenza, sostengono l'attuazione dei controlli, promuovono la consapevolezza del personale e garantiscono la gestione delle evidenze documentate. Tutto il personale e i collaboratori sono tenuti ad operare secondo ruoli, autorizzazioni e responsabilità formalmente assegnate.

5.2 Funzioni aziendali censite

Funzione	Scopo	Responsabilità	Attività
Direzione	Definire indirizzi, priorita e supervisione generale dell'organizzazione.	Governance aziendale, approvazione decisioni, riesame obiettivi e supervisione del sistema di gestione.	Pianificazione strategica, approvazioni, coordinamento dei responsabili, monitoraggio risultati.
Amministrazione	Gestire aspetti amministrativi, contabili e documentali dell'organizzazione.	Contabilita, scadenze amministrative, gestione documentazione economico-amministrativa.	Registrazioni contabili, gestione pagamenti, archiviazione documenti amministrativi.
Risorse Umane	Gestire personale, ruoli, inserimenti e aspetti organizzativi connessi alle persone.	Anagrafica personale, onboarding, gestione ruoli e coordinamento esigenze formative.	Aggiornamento organigramma, raccolta dati personale, gestione comunicazioni HR.
IT	Supportare sistemi informativi, strumenti digitali e continuita operativa tecnologica.	Gestione infrastruttura IT, supporto utenti, sicurezza tecnica di base e continuita operativa.	Assistenza tecnica, gestione account, backup, presidio dei sistemi e delle dotazioni informatiche.
Sicurezza delle informazioni	Presidiare aspetti organizzativi e operativi relativi alla sicurezza delle informazioni.	Coordinamento SGSI, verifica controlli, gestione miglioramenti e supporto alla conformita.	Analisi rischi, aggiornamento controlli, supporto SoA, monitoraggio azioni di trattamento.
Commerciale	Gestire relazioni commerciali, clienti, offerte e sviluppo opportunita.	Gestione clienti, offerte, sviluppo commerciale e mantenimento relazioni.	Contatti commerciali, preventivi, aggiornamento opportunita e coordinamento richieste clienti.
Operations	Coordinare l'operativita corrente e l'erogazione dei servizi o delle attivita principali.	Pianificazione operativa, assegnazione attivita, monitoraggio esecuzione e continuita operativa.	Coordinamento operativo, pianificazione attivita, controllo

Funzione	Scopo	Responsabilità	Attività
			avanzamento e gestione priorita.
Qualita e Compliance	Supportare conformita, procedure, controlli documentali e miglioramento continuo.	Gestione procedure, verifiche interne, conformita normativa e presidio documentale.	Aggiornamento documenti, raccolta evidenze, verifica attuazione procedure e supporto audit.

5.3 Persone e ruoli censiti

Nominativo	Ruolo	Funzione	Responsabile diretto	Stato
Gilda Gangemi	Amministrazione	Amministrazione	Michele Pietravalle	Attivo
Michele Pietravalle	Legale Rappresentante	Direzione		Attivo

5.4 Risorse e competenze

Le risorse necessarie in termini di persone, competenze, tecnologie, budget e supporto operativo sono pianificate in modo coerente con priorità di rischio, obblighi di conformità e obiettivi del business.

5.5 Comunicazione

I flussi informativi interni ed esterni relativi al SGSI sono stabiliti per garantire tempestività, tracciabilità, adeguata autorizzazione e corretta gestione delle evidenze documentate.

6. SEDI, UNITÀ ORGANIZZATIVE E AMBIENTI INCLUSI

Sito	Indirizzo	Paese	Note
DataCenter Milano Caldera	via Caldera 21 Milano	Italia	c/o Seeweb
DataCenter Milano MIX	via Caldera 21 Milano	Italia	c/o MIX
Laboratorio	via dei Giuliani 8/b Trieste	Italia	
Sede Legale	P.le L.da vinci 8/e/4 Venezia	Italia	Sede Legale senza attività operativa

Numero siti/ambienti censiti nel perimetro: **4**.

7. ASSET INFORMATIVI E CRITERI DI CLASSIFICAZIONE

Gli asset del SGSI comprendono informazioni, servizi, applicazioni, infrastrutture, dispositivi, archivi documentali, risorse umane, sedi e altri elementi di supporto al business. Ciascun asset deve essere identificato, associato a un owner, classificato secondo i requisiti di riservatezza, integrità e disponibilità e gestito lungo il relativo ciclo di vita.

7.1 Criteri di classificazione

La classificazione degli asset e delle informazioni considera criticità per il business, requisiti contrattuali, impatti legali/regolatori e conseguenze operative in caso di compromissione o indisponibilità.

Asset	Tipo	Owner	C	I	A	Note
Archivio documenti societari	Archivio cartaceo	Amministrazione / Direzione	4	3	2	Contengono contratti, documenti HR, atti societari o registrazioni sensibili in formato cartaceo.
BGP_MIL02-MIX S/N 2102353AES10N3100076	Router	Responsabile IT	4	5	4	Router BGP ridondato per erogazione servizi IP Transit ai clienti
Caselle e-mail aziendali	Servizio Private Cloud	Responsabile IT	4	4	4	Utilizzate per comunicazioni interne, esterne, invio documenti e gestione credenziali di servizi terzi.
Dispositivi mobili aziendali	Dispositivo mobile	Responsabile IT	5	1	2	Smartphone e tablet con accesso a posta, file, autenticazione e applicazioni aziendali.
Documenti contrattuali e amministrativi	Documentazione	Amministrazione / Direzione	4	4	3	Documentazione rilevante ai fini legali, fiscali, organizzativi e di conformità.
MIL01-BGP-SW	Infrastruttura	Responsabile IT	4	4	4	Router BGP ridondato per erogazione servizi IP Transit ai clienti
MIL01-FW1	Infrastruttura	Responsabile IT	3	5	5	Firewall ridondati centralizzati. Proteggono segmentazione, connettività, accessi remoti e perimetro di rete aziendale e dei clienti,

Asset	Tipo	Owner	C	I	A	Note
MIL01-IR1A/B	Infrastruttura	Responsabile IT	4	4	4	Router accesso ridondato per erogazione servizi IP Access ai clienti
MIL01-Storage01	Infrastruttura	Responsabile IT	4	4	4	Storage ridondato
MIL01-Storage02	Infrastruttura	Responsabile IT	4	4	4	Storage ridondato
MIL01-SWITCH1	Stacked Switch	Responsabile IT	4	4	4	Switch stacked ridondato per erogazione servizi network
NextCloud	Private Cloud workspace	Responsabile IT	4	4	4	Suite cloud per collaborazione, documenti, calendari, videoconferenze e condivisione file.
PC e laptop dipendenti	Endpoint	Responsabili di funzione	4	4	4	Strumenti di lavoro con accesso a dati, servizi cloud, documentazione e sistemi aziendali.
Qnap Backup Caldera	Backup	Responsabile IT	4	5	5	Copie di sicurezza necessarie al ripristino in caso di incidente, errore umano o attacco informatico.
Qnap Backup Trieste	Backup	Responsabile IT	5	5	5	Copie di sicurezza offsite necessarie al ripristino in caso di incidente, errore umano o attacco informatico.
Server / infrastruttura virtuale	Infrastruttura	Responsabile IT	4	5	5	Ospita applicazioni, dati e servizi essenziali per l’operatività aziendale e la continuità del business.
Sito web aziendale	Sito web	Marketing / IT	2	4	4	Canale istituzionale e commerciale, importante per immagine, reputazione e

Asset	Tipo	Owner	C	I	A	Note
						continuità di contatto con il mercato.

Legenda CIA: Confidenzialità, Integrità, Disponibilità. Numero asset censiti nel perimetro: **17**.

8. METODOLOGIA DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO

8.1 Metodologia di valutazione dei rischi

L’organizzazione adotta una metodologia strutturata di risk assessment e risk treatment che prende in considerazione contesto, asset, minacce, vulnerabilità, probabilità, impatto e livello di rischio risultante. I criteri di accettazione del rischio, le priorità di intervento e le decisioni di trattamento sono definiti in modo coerente con gli obiettivi di business, la propensione al rischio dell’organizzazione, gli obblighi applicabili e le capacità operative disponibili.

8.2 Opzioni di trattamento

Le opzioni di trattamento includono riduzione, trasferimento, evitamento o accettazione motivata del rischio. La metodologia viene aggiornata quando intervengono cambiamenti rilevanti nel contesto, nel perimetro, nelle tecnologie, nei processi, nei requisiti contrattuali o nel panorama delle minacce.

9. QUADRO DEI RISCHI E PRIORITÀ DI INTERVENTO

9.1 Report di valutazione del rischio

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
Caselle e-mail aziendali	Phishing e compromissione account	Formazione insufficiente, MFA assente, filtri antispam non adeguati	16	Critico	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights; A.6.3 Information security awareness, education and training; A.5.10 Acceptable use of information and other associated assets.
MIL01-Storage02	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
MIL01-Storage01	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
MIL01-BGP-SW	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
MIL01-IR1A/B	Malware, ransomware o	Patching incompleto,	15	Critico	Mitigare il rischio con patch management, protezioni

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
	indisponibilità infrastrutturale	hardening insufficiente o monitoraggio debole			endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
NextCloud	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
MIL01-FW1	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
Qnap Backup Caldera	Impossibilità di ripristino	Backup non testati o retention inadeguata	15	Critico	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity.
Server / infrastruttura virtuale	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
Qnap Backup Trieste	Impossibilità di ripristino	Backup non testati o retention inadeguata	15	Critico	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
					backup; A.5.30 ICT readiness for business continuity.
Dispositivi mobili aziendali	Smarrimento o furto del dispositivo	Cifratura disco assente o controllo remoto non attivo	12	Alto	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.
PC e laptop dipendenti	Smarrimento o furto del dispositivo	Cifratura disco assente o controllo remoto non attivo	12	Alto	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.

Numero complessivo dei rischi registrati: **17**.

10. OBIETTIVI SGSI, PIANIFICAZIONE E RISORSE

Gli obiettivi del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni comprendono:
garantire la riservatezza, integrità e disponibilità delle informazioni aziendali e dei dati dei clienti;
ridurre il rischio di incidenti di sicurezza informatica e interruzioni operative;
assicurare continuità e affidabilità dei servizi ICT e di telecomunicazione erogati;
migliorare continuamente i processi aziendali e l'efficacia dei controlli di sicurezza;
monitorare e mitigare tempestivamente minacce cyber, vulnerabilità e attacchi DDoS;
garantire adeguati livelli di backup, disaster recovery e resilienza infrastrutturale;
assicurare la conformità ai requisiti normativi, contrattuali e agli standard ISO applicabili;
migliorare la soddisfazione del cliente attraverso qualità, affidabilità e sicurezza dei servizi;
promuovere consapevolezza e formazione continua del personale sui temi qualità e sicurezza delle informazioni;
mantenere elevati standard di monitoraggio, tracciabilità e gestione degli accessi ai sistemi aziendali.

Gli obiettivi del SGSI devono essere misurabili ove possibile, coerenti con la politica per la sicurezza delle informazioni, assegnati a responsabili identificati, monitorati tramite indicatori e riesaminati periodicamente. L'organizzazione garantisce risorse adeguate in termini di persone, competenze, tecnologie, budget, tempo e supporto operativo per l'attuazione delle iniziative di sicurezza.

11. CONTROLLI, STATEMENT OF APPLICABILITY E PIANO DI TRATTAMENTO

11.1 Controlli e SoA

I controlli del SGSI sono determinati in funzione dei risultati dell'analisi del rischio, dei requisiti applicabili e delle esigenze operative dell'organizzazione. La Statement of Applicability formalizza per ciascun controllo la decisione di applicabilità, lo stato di implementazione e la relativa motivazione.

11.2 Piano di trattamento del rischio

Il piano di trattamento traduce i rischi significativi in azioni, responsabilità, scadenze e stati di avanzamento, mantenendo coerenza tra rischio, controllo, responsabili e capacità attuativa del business.

Controlli applicabili o da confermare presenti in archivio: **33**. Azioni/piani di trattamento presenti: **17**. Procedure SGSI registrate: **8**.

12. COMPETENZA, CONSAPEVOLEZZA, COMUNICAZIONE E CONTROLLO DOCUMENTALE

12.1 Competenze e consapevolezza

L’organizzazione assicura che il personale operi con adeguata competenza e consapevolezza rispetto a ruoli, responsabilità, politiche, procedure e requisiti di sicurezza.

12.2 Controllo documentale

Le informazioni documentate del SGSI sono identificate, approvate, aggiornate, protette, rese disponibili e conservate in modo controllato per garantirne integrità, reperibilità e adeguatezza d’uso. Le comunicazioni interne ed esterne rilevanti per il SGSI sono pianificate, tracciate quando necessario e gestite secondo criteri di riservatezza e autorizzazione.

13. GESTIONE OPERATIVA, MONITORAGGIO E RISPOSTA AGLI EVENTI

13.1 Attuazione operativa

Le attività operative del SGSI comprendono l’attuazione dei controlli, la gestione dei cambiamenti, il monitoraggio delle misure di sicurezza, il presidio delle vulnerabilità, la gestione degli incidenti e la conservazione delle evidenze.

13.2 Risposta agli eventi e non conformità

Eventi, anomalie, non conformità e incidenti informativi devono essere rilevati, registrati, valutati, trattati e, ove opportuno, analizzati per identificarne cause, impatti e azioni correttive.

14. AUDIT INTERNI, RIESAME DELLA DIREZIONE E MIGLIORAMENTO CONTINUO

14.1 Audit e riesame

Il SGSI è sottoposto a audit interni pianificati, riesami periodici della Direzione e verifiche dell’efficacia delle misure adottate.

14.2 Miglioramento continuo

I risultati di audit, monitoraggi, incidenti, analisi dei rischi, trattamenti, indicatori e feedback delle parti interessate alimentano il processo di miglioramento continuo. Le azioni correttive e di miglioramento devono essere proporzionate ai rilievi emersi, assegnate a responsabili identificati e verificate fino alla loro chiusura.

15. ALLEGATI E DOCUMENTI CORRELATI

Il presente manuale si integra con il registro degli asset, il registro dei rischi, il piano di trattamento del rischio, la Statement of Applicability, la politica per la sicurezza delle informazioni, le procedure operative e ogni altra informazione documentata del SGSI rilevante ai fini del governo, della conformità e dell’efficacia del sistema.