SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Gestione asset informativi

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	PROC-AST-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.

PROC-AST-001 - GESTIONE ASSET INFORMATIVI

Procedura Gestione asset informativi

Scopo
Stabilire regole operative coerenti con il SGSI di NetJoin S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivio documenti societari (Archivio cartaceo)
- BGP_MIL02-MIX S/N 2102353AES10N3100076 (Router)
- Caselle e-mail aziendali (Servizio Private Cloud)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- MIL01-BGP-SW (Infrastruttura)
- MIL01-FW1 (Infrastruttura)
- MIL01-IR1A/B (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- MIL01-Storage02: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- MIL01-Storage01: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- MIL01-BGP-SW: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- MIL01-IR1A/B: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- NextCloud: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- MIL01-FW1: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Qnap Backup Caldera: Impossibilità di ripristino [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per MIL01-SWITCH1, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per BGP_MIL02-MIX S/N 2102353AES10N3100076, con owner Responsabile IT e presidio del controllo

Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Archivio documenti societari, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Dispositivi mobili aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.