SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

# Manuale SGSI

DNS Informatica S.a.s. di Marco Racca & C. è una società italiana operante dal 2000 nel settore dei servizi e delle soluzioni IT e ICT. L'organizzazione affianca aziende, piccole e medie imprese, enti pubblici e studi professionali nella progettazione, realizzazione, gestione e protezione delle rispettive infrastrutture informatiche, adottando un approccio consulenziale, proattivo e orientato alle specifiche esigenze del cliente.

L'azienda opera come partner tecnologico per la fornitura di servizi gestiti e soluzioni chiavi in mano, comprendenti sistemistica, cloud computing, hosting, cybersecurity, telefonia IP e comunicazioni unificate, assistenza tecnica remota, IT management, assessment, programmazione informatica, manutenzione di computer e periferiche e gestione delle infrastrutture tecnologiche. DNS Informatica si avvale di personale e collaboratori con competenze specialistiche e certificazioni su tecnologie e sistemi multipiattaforma.

| | |
|---|---|
| **Codice** | SGSI-MAN-001 |
| **Data documento** | 20/07/2026 |
| **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

DNS Informatica S.a.s. di Marco Racca & C. è una società italiana operante dal 2000 nel settore dei servizi e delle soluzioni IT e ICT. L'organizzazione affianca aziende, piccole e medie imprese, enti pubblici e studi professionali nella progettazione, realizzazione, gestione e protezione delle rispettive infrastrutture informatiche, adottando un approccio consulenziale, proattivo e orientato alle specifiche esigenze del cliente.

L'azienda opera come partner tecnologico per la fornitura di servizi gestiti e soluzioni chiavi in mano, comprendenti sistemistica, cloud computing, hosting, cybersecurity, telefonia IP e comunicazioni unificate, assistenza tecnica remota, IT management, assessment, programmazione informatica, manutenzione di computer e periferiche e gestione delle infrastrutture tecnologiche. DNS Informatica si avvale di personale e collaboratori con competenze specialistiche e certificazioni su tecnologie e sistemi multipiattaforma.

## DESCRIZIONE DEL SERVIZIO

Il servizio comprende l'analisi dei requisiti tecnologici, organizzativi e di sicurezza del cliente, la progettazione e configurazione delle soluzioni, l'installazione, la migrazione, la gestione, la manutenzione, il monitoraggio e l'assistenza delle infrastrutture IT e ICT.

In funzione delle esigenze e degli accordi contrattuali con il cliente, il servizio può comprendere:

assessment dell'infrastruttura e dei processi informatici;
progettazione e gestione di server, reti, postazioni di lavoro e periferiche;
fornitura, configurazione e manutenzione di hardware e software;
gestione sistemistica e outsourcing completo o parziale dell'infrastruttura IT;
servizi cloud, hosting, server virtuali, posta elettronica e sistemi di collaborazione;
backup, protezione dei dati e supporto alle attività di ripristino;
soluzioni di cybersecurity, protezione degli endpoint, monitoraggio e gestione degli eventi di sicurezza;
telefonia IP, centralini cloud e sistemi di comunicazione unificata;
assistenza tecnica remota e interventi presso le sedi dei clienti;
programmazione informatica, integrazione e personalizzazione di applicazioni;
videosorveglianza, IoT, controllo degli accessi e soluzioni tecnologiche correlate;
noleggio operativo di apparati e infrastrutture informatiche;
gestione, riparazione e manutenzione di computer e periferiche.

I servizi sono erogati con l'obiettivo di assicurare continuità operativa, affidabilità, disponibilità dei sistemi e adeguata protezione delle informazioni. Le attività sono svolte nel rispetto degli accordi contrattuali, delle responsabilità assegnate, dei livelli di servizio concordati e dei requisiti applicabili in materia di riservatezza, integrità, disponibilità e protezione dei dati.

## 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 DNS INFORMATICA S.A.S. di MARCO RACCA & C. 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

DNS Informatica S.a.s. di Marco Racca & C. è una società italiana operante dal 2000 nel settore dei servizi e delle soluzioni IT e ICT. L'organizzazione affianca aziende, piccole e medie imprese, enti pubblici e studi professionali nella progettazione, realizzazione, gestione e protezione delle rispettive infrastrutture informatiche, adottando un approccio consulenziale, proattivo e orientato alle specifiche esigenze del cliente.

L'azienda opera come partner tecnologico per la fornitura di servizi gestiti e soluzioni chiavi in mano, comprendenti sistemistica, cloud computing, hosting, cybersecurity, telefonia IP e comunicazioni unificate, assistenza tecnica remota, IT management, assessment, programmazione informatica, manutenzione di computer e periferiche e gestione delle infrastrutture tecnologiche. DNS Informatica si avvale di personale e collaboratori con competenze specialistiche e certificazioni su tecnologie e sistemi multipiattaforma.

### 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 per la Sicurezza delle Informazioni di DNS Informatica S.a.s. di Marco Racca & C. si applica alla progettazione, fornitura, configurazione, installazione, gestione, monitoraggio, manutenzione e assistenza di infrastrutture, sistemi e servizi IT e ICT destinati ad aziende, piccole e medie imprese, enti pubblici e studi professionali.

Il perimetro comprende, in particolare, i servizi di sistemistica, gestione di server e reti, cloud computing, hosting, cybersecurity, backup e ripristino, telefonia IP e comunicazioni unificate, assistenza tecnica remota e on-site, IT management, assessment tecnologico, programmazione informatica, manutenzione di computer e periferiche e fornitura di infrastrutture informatiche. Tali attività sono coerenti con i servizi dichiarati dall'organizzazione e con le attività risultanti dalla documentazione camerale.

Sono compresi nello scopo:

i processi direzionali e di pianificazione strategica;
la gestione commerciale e la raccolta dei requisiti dei clienti;
la progettazione e configurazione delle soluzioni;
l'approvvigionamento e la gestione dei fornitori;
l'erogazione dei servizi gestiti e delle attività di assistenza;
la gestione dei ticket, degli interventi e delle richieste dei clienti;
il monitoraggio delle infrastrutture e degli eventi di sicurezza;
la gestione degli incidenti, delle vulnerabilità e delle modifiche;
la gestione degli accessi, degli account e dei privilegi;
la gestione degli asset hardware, software, informativi e cloud;
il backup, il ripristino e la continuità operativa;
la gestione documentale, amministrativa e contrattuale;
la gestione delle competenze, della formazione e delle responsabilità del personale;
la valutazione dei rischi e il miglioramento continuo del SGSI.

Il perimetro organizzativo comprende l'Alta Direzione, il personale tecnico, la funzione commerciale, le funzioni amministrative e gli eventuali collaboratori e fornitori esterni che accedono alle informazioni, ai sistemi o alle infrastrutture comprese nello scopo.

Il perimetro fisico comprende:

sede legale: Via Ticino 51, 28068 Romentino (NO);
sede operativa e unità locale: Via Pietro Micca 3, 28069 Trecate (NO);
postazioni di lavoro remoto autorizzate;
infrastrutture e servizi ospitati presso data center, ambienti cloud e fornitori esterni contrattualizzati.

La sede operativa di Trecate è registrata come ufficio e sede operativa per lo svolgimento di servizi connessi alle tecnologie informatiche, gestione di strutture informatiche, programmazione, manutenzione e fornitura di infrastrutture e hosting.

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

DNS Informatica adotta una struttura organizzativa snella, nella quale l'Alta Direzione mantiene il coordinamento generale delle attività, delle risorse, delle relazioni commerciali e delle decisioni strategiche. L'organizzazione opera attraverso personale tecnico e commerciale e può avvalersi di collaboratori e fornitori specializzati.

Le attività aziendali richiedono competenze multidisciplinari in materia di sistemistica, networking, cloud, hosting, cybersecurity, assistenza remota, telefonia IP, programmazione, manutenzione e gestione delle infrastrutture. Il sito aziendale dichiara la disponibilità di personale e collaboratori certificati su tecnologie multipiattaforma e l'erogazione di soluzioni personalizzate e servizi chiavi in mano.

I principali fattori interni rilevanti per il SGSI sono:

concentrazione di alcune responsabilità direzionali e operative su un numero limitato di persone;
necessità di formalizzare ruoli, deleghe, responsabilità e sostituzioni;
elevato livello di privilegi tecnici necessari per amministrare sistemi propri e dei clienti;
utilizzo di strumenti di collegamento e assistenza remota;
trattamento di configurazioni, credenziali, log, backup e informazioni tecniche dei clienti;
dipendenza dalle competenze specialistiche del personale tecnico;
necessità di garantire aggiornamento professionale e formazione continua;
utilizzo di piattaforme cloud e servizi esterni per l'erogazione delle attività;
gestione contemporanea di infrastrutture eterogenee e multipiattaforma;
necessità di mantenere inventari aggiornati di asset, software, licenze, account e servizi;
esigenza di assicurare separazione dei compiti e controllo delle attività privilegiate;
necessità di documentare configurazioni, interventi, modifiche e incidenti;
dipendenza dalla disponibilità delle connessioni, degli strumenti di monitoraggio e dei sistemi di assistenza;
esigenza di garantire continuità operativa anche in caso di indisponibilità di personale, sede, sistemi o fornitori;
necessità di integrare il SGSI nelle ordinarie attività tecniche e commerciali senza rallentare l'erogazione dei servizi.

Tra i punti di forza interni si considerano l'esperienza maturata dal 2000, la conoscenza delle infrastrutture dei clienti, la capacità di offrire servizi personalizzati, la disponibilità di competenze tecniche specialistiche e la possibilità di intervenire da remoto o presso le sedi dei clienti.

### 4.2 Analisi del contesto esterno

DNS Informatica opera in un mercato tecnologico caratterizzato da una rapida evoluzione delle minacce informatiche, delle soluzioni cloud, delle tecnologie di comunicazione e delle aspettative dei clienti in termini di continuità, tempestività e protezione dei dati.

I principali fattori esterni rilevanti sono:

aumento della frequenza e della complessità di ransomware, phishing, furto di credenziali, compromissione degli account e attacchi alla supply chain;
rapida obsolescenza delle tecnologie e necessità di aggiornare costantemente competenze, prodotti e configurazioni;
crescente dipendenza da provider cloud, hosting, telecomunicazioni, software, hardware e servizi di sicurezza;
possibili interruzioni, vulnerabilità o modifiche contrattuali dei servizi forniti da terze parti;

richieste dei clienti relative a SLA, tempi di intervento, reperibilità, riservatezza e continuità operativa;
necessità di rispettare i requisiti contrattuali e di proteggere le informazioni affidate dai clienti;
obblighi applicabili in materia di protezione dei dati personali, sicurezza informatica, proprietà intellettuale, licenze software, conservazione documentale e rapporti di lavoro;
eventuali requisiti derivanti dal GDPR, dalla normativa nazionale sulla protezione dei dati, dalla disciplina NIS2 e dalle disposizioni dell'Autorità nazionale competente, quando applicabili all'organizzazione o ai clienti serviti;
aspettative di clienti pubblici e privati riguardo alla qualificazione dei fornitori e alla dimostrazione di controlli di sicurezza adeguati;
concorrenza di operatori nazionali, fornitori cloud globali e società di servizi gestiti;
difficoltà di reperimento e mantenimento di personale tecnico qualificato;
dipendenza dalla disponibilità di energia elettrica, connettività Internet, reti telefoniche e infrastrutture dei data center;
rischi fisici e ambientali che possono interessare le sedi o le infrastrutture dei fornitori;
evoluzione delle tecniche di intelligenza artificiale e automazione, utilizzabili sia per migliorare i servizi sia per realizzare nuove forme di attacco.

Il mercato di riferimento comprende aziende, PMI, enti pubblici e studi professionali, ai quali DNS Informatica offre servizi gestiti e assistenza specialistica, escludendo ordinariamente il mercato dei clienti privati.

**4.3 Parti interessate e relative esigenze**

Alta Direzione e soci

Si aspettano tutela della reputazione aziendale, continuità dei ricavi, protezione del patrimonio informativo, rispetto delle norme, controllo dei rischi, sostenibilità economica del SGSI e disponibilità di informazioni attendibili per assumere decisioni.

Dipendenti e collaboratori

Si aspettano ruoli e responsabilità chiari, strumenti affidabili, accessi adeguati alle mansioni, formazione, supporto, protezione dei dati personali, sicurezza degli ambienti di lavoro e procedure applicabili e comprensibili.

Clienti e relativi utenti

Si aspettano riservatezza delle informazioni, integrità delle configurazioni e dei dati, disponibilità dei servizi, tempestività dell'assistenza, rispetto degli SLA, protezione delle credenziali, tracciabilità degli interventi, continuità operativa e comunicazione tempestiva in caso di incidente.

Enti pubblici clienti

Si aspettano conformità normativa, protezione delle informazioni, affidabilità dei servizi, tracciabilità delle attività, rispetto degli obblighi contrattuali, continuità e adeguate misure di sicurezza da parte del fornitore.

Fornitori cloud, hosting, telecomunicazioni e software

Si aspettano rispetto delle condizioni contrattuali e di licenza, utilizzo corretto dei servizi, protezione degli account, comunicazione degli incidenti e collaborazione nella gestione delle vulnerabilità e delle interruzioni.

Fornitori di hardware e apparati

Si aspettano corretta gestione degli ordini, dei prodotti, delle garanzie, delle licenze e delle informazioni commerciali condivise.

Partner e subfornitori tecnici

Si aspettano definizione delle responsabilità, autorizzazioni chiare, accessi limitati, requisiti di sicurezza formalizzati, protezione delle informazioni ricevute e rispetto degli accordi di riservatezza.

Autorità e organismi di controllo

Si aspettano conformità alle disposizioni applicabili, disponibilità delle registrazioni, collaborazione in caso di verifica e gestione corretta delle notifiche e degli incidenti soggetti a obblighi di comunicazione.

Interessati al trattamento dei dati personali

Si aspettano liceità, correttezza, trasparenza, protezione dei dati, limitazione degli accessi, rispetto dei tempi di conservazione e gestione dei diritti previsti dalla normativa.

Organismo di certificazione e auditor

Si aspettano evidenze oggettive dell'attuazione del SGSI, disponibilità della documentazione, gestione delle non conformità, indipendenza delle verifiche e impegno al miglioramento continuo.

Comunità e territorio

Si aspettano comportamento responsabile, continuità dell'attività, riduzione degli impatti ambientali, corretto smaltimento delle apparecchiature e impiego consapevole delle tecnologie.

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 |
|---|---|---|---|---|
| Alberto Bertozzi | Sales Manager | Commerciale | | Attivo |
| Luca Giannotta | Tecnico Infrastrutture e Networking | Sicurezza delle informazioni | Marco Racca | Attivo |
| Marco Racca | Socio accomandatario | Amministrazione | | Attivo |
| Miriam Martelli | Socio accomandante | Amministrazione | | Attivo |
| Simone Di Belardino | componente tecnico del team DNS Informatica, con competenze in cybersecurity, sicurezza delle reti e disaster recover | IT | Marco Racca | 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 |
|---|---|---|---|
| Nessuna sede censita. | | | |

Numero siti/ambienti censiti nel perimetro: **0**.

## 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 |
|---|---|---|---|---|---|---|
| Archivi cartacei riservati | Archivio cartaceo | Amministrazione / Direzione | 4 | 3 | 2 | Contengono contratti, documenti HR, atti societari o registrazioni sensibili in formato cartaceo. |
| Backup aziendali | Backup | Responsabile IT | 4 | 5 | 5 | Copie di sicurezza necessarie al ripristino in caso di incidente, errore umano o attacco informatico. |
| Caselle e-mail aziendali | Servizio SaaS | Responsabile IT | 4 | 4 | 4 | Utilizzate per comunicazioni interne, esterne, invio documenti e gestione credenziali di servizi terzi. |
| CRM / ERP | Applicazione | Responsabile di processo | 4 | 5 | 4 | Sistema gestionale usato per processi commerciali, amministrativi e decisionali. |
| Database clienti | Database | Responsabile commerciale / IT | 5 | 5 | 4 | Contiene dati personali, storici ordini, offerte, contatti commerciali e informazioni riservate. |
| Dispositivi mobili aziendali | Dispositivo mobile | Responsabile IT | 4 | 4 | 3 | 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. |
| Firewall e apparati di rete | Infrastruttura | Responsabile IT | 3 | 5 | 5 | Proteggono segmentazione, connettività, accessi remoti e perimetro di rete aziendale. |
| PC e laptop dipendenti | Endpoint | Responsabili di funzione | 3 | 4 | 4 | Strumenti di lavoro con accesso a dati, servizi cloud, |

| Asset | Tipo | Owner | C | I | A | Note |
|---|---|---|---|---|---|---|
| | | | | | | documentazione e sistemi aziendali. |
| Piattaforma documentale / DMS | Applicazione | Qualità / IT | 4 | 5 | 4 | Raccoglie manuali, procedure, registrazioni, versioni e approvazioni documentali. |
| Portale clienti / area riservata | Sito web | Responsabile IT / Commerciale | 4 | 5 | 4 | Espone funzionalità applicative o documentali a clienti e partner attraverso autenticazione. |
| Server / infrastruttura virtuale | Infrastruttura | Responsabile IT | 4 | 5 | 5 | Ospita applicazioni, dati e servizi essenziali per l'operatività aziendale e la continuità del business. |
| Sistema HR / anagrafiche personale | Applicazione | HR | 5 | 4 | 3 | Gestisce dati del personale, ruoli, documenti, presenze e informazioni soggette a riservatezza elevata. |
| Sito web aziendale | Sito web | Marketing / IT | 2 | 4 | 4 | Canale istituzionale e commerciale, importante per immagine, reputazione e continuità di contatto con il mercato. |
| Workspace cloud collaborativo | Cloud workspace | Responsabile IT | 4 | 4 | 4 | Suite cloud per collaborazione, documenti, calendari, videoconferenze e condivisione file. |

Legenda CIA: Confidenzialità, Integrità, Disponibilità. Numero asset censiti nel perimetro: **15**.

## 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 |
|---|---|---|---|---|---|
| Server / infrastruttura virtuale | Diffusione malware / ransomware | Sistemi non aggiornati o protezioni endpoint insufficienti | 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. |
| Database clienti | Perdita o indisponibilità dei dati | Backup assenti o non verificati | 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. |
| Database clienti | Modifica non autorizzata dei dati | Permessi eccessivi o assenza di tracciamento log | 12 | Alto | 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. |
| Database clienti | Violazione della confidenzialità delle informazioni | Classificazione dati assente o canali di invio non protetti | 12 | Alto | Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. |
| Database clienti | Errore umano nella gestione documenti o dati | Procedure non formalizzate o formazione insufficiente | 12 | Alto | Mitigare il rischio formalizzando istruzioni operative, verifiche a campione e formazione periodica al personale. Controlli suggeriti: A.6.3 Information security awareness, education and training; A.5.10 Acceptable use of information and other associated assets. |
| Database clienti | Accesso non autorizzato ai | Password deboli o | 12 | Alto | Mitigare il rischio applicando il principio del minimo privilegio, |

| Asset | Minaccia | Vulnerabilità | Score | Livello | Trattamento |
|---|---|---|---|---|---|
| | dati | mancata MFA | | | 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. |

Numero complessivo dei rischi registrati: **8**.

## 10. OBIETTIVI SGSI, PIANIFICAZIONE E RISORSE

DNS Informatica stabilisce i seguenti obiettivi per la sicurezza delle informazioni. Gli obiettivi sono monitorati periodicamente e riesaminati almeno annualmente dall'Alta Direzione.

Obiettivo Indicatore Traguardo
Mantenere aggiornato l'inventario degli asset Asset identificati, classificati e assegnati a un responsabile 100% degli asset critici
Proteggere gli account privilegiati Account amministrativi protetti mediante autenticazione multifattore, ove tecnicamente disponibile 100%
Ridurre l'esposizione alle vulnerabilità Vulnerabilità critiche corrette o formalmente trattate Entro 15 giorni
Gestire tempestivamente le vulnerabilità elevate Vulnerabilità elevate corrette o formalmente trattate Entro 30 giorni
Garantire l'efficacia dei backup Processi di backup critici completati con esito positivo Almeno 98%
Verificare la capacità di ripristino Test documentati di ripristino dei sistemi e dati critici Almeno uno ogni trimestre
Migliorare la consapevolezza del personale Personale che completa la formazione annuale sulla sicurezza 100%
Ridurre il rischio di phishing Personale sottoposto ad almeno una simulazione o verifica annuale 100%
Garantire la gestione degli incidenti Incidenti registrati, classificati e presi in carico secondo la procedura 100%
Ridurre la reiterazione degli incidenti Incidenti rilevanti sottoposti ad analisi delle cause 100%
Controllare i fornitori critici Fornitori critici valutati o riesaminati sotto il profilo della sicurezza 100% ogni anno
Controllare gli accessi Account e privilegi sottoposti a riesame formale Almeno semestrale
Revocare tempestivamente gli accessi Accessi revocati dopo cessazione o cambio di mansione Entro un giorno lavorativo
Verificare la conformità del SGSI Audit interno completo del sistema Almeno uno ogni anno
Garantire il governo del sistema Riesame del SGSI da parte dell'Alta Direzione Almeno uno ogni anno
Gestire le non conformità Non conformità con responsabile, azione e scadenza definiti 100%
Migliorare la continuità operativa Esecuzione di una prova del piano di continuità o disaster recovery Almeno una volta all'anno
Migliorare il monitoraggio Sistemi e servizi critici coperti da monitoraggio e allerta 100%
Migliorare la soddisfazione del cliente Reclami relativi a sicurezza e indisponibilità analizzati e trattati 100%
Proteggere le informazioni dei clienti Incidenti gravi imputabili a mancata applicazione di controlli approvati Obiettivo: zero

L'Alta Direzione assegna per ciascun obiettivo un responsabile, le risorse necessarie, la frequenza di misurazione e le modalità di rendicontazione. Gli eventuali scostamenti sono analizzati e gestiti mediante azioni correttive o piani di miglioramento.

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: **28**. Azioni/piani di trattamento presenti: **7**. 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.