

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Politica Sicurezza Informazioni

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 multiplatforma.

Codice	SGSI-POL-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

Impegno della direzione
Principi di riferimento
Campo di applicazione
Obiettivi
Responsabilità organizzative
Riesame

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.

IMPEGNO DELLA DIREZIONE

La Direzione di DNS INFORMATICA S.A.S. di MARCO RACCA & C. si impegna a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni, garantendo risorse adeguate, responsabilità chiare e monitoraggio dell'efficacia del SGSI.

PRINCIPI DI RIFERIMENTO

- approccio basato sul rischio;
- principio del minimo privilegio;
- separazione dei compiti;
- controllo dei fornitori e dei servizi cloud;
- formazione continua del personale;
- gestione tempestiva degli incidenti.

CAMPO DI APPLICAZIONE

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.

OBIETTIVI

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.

RESPONSABILITÀ ORGANIZZATIVE

L’attuazione della presente politica è sostenuta dalle funzioni aziendali e dai ruoli censiti in piattaforma. I responsabili di funzione, gli owner dei processi e il personale incaricato contribuiscono al mantenimento del SGSI in coerenza con le responsabilità formalmente assegnate.

Funzione	Responsabilità
Direzione	Governance aziendale, approvazione decisioni, riesame obiettivi e supervisione del sistema di gestione.
Amministrazione	Contabilità, scadenze amministrative, gestione documentazione economico-amministrativa.
Risorse Umane	Anagrafica personale, onboarding, gestione ruoli e coordinamento esigenze formative.
IT	Gestione infrastruttura IT, supporto utenti, sicurezza tecnica di base e continuità operativa.
Sicurezza delle informazioni	Coordinamento SGSI, verifica controlli, gestione miglioramenti e supporto alla conformità.
Commerciale	Gestione clienti, offerte, sviluppo commerciale e mantenimento relazioni.
Operations	Pianificazione operativa, assegnazione attività, monitoraggio esecuzione e continuità operativa.
Qualità e Compliance	Gestione procedure, verifiche interne, conformità normativa e presidio documentale.

RIESAME

La presente politica è riesaminata periodicamente, in occasione di modifiche organizzative rilevanti, incidenti significativi o aggiornamenti normativi e contrattuali.