SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

# Procedure 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-PRC-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

Pack procedure SGSI

## 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. |

## PACK PROCEDURE SGSI

Le procedure riportate di seguito definiscono i controlli operativi minimi per la gestione del SGSI.

**PROC-BCK-001 - Backup e ripristino**

Procedura Backup e ripristino

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-CLS-001 - Classificazione delle informazioni**

Procedura Classificazione delle informazioni

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-BCP-001 - Continuità operativa e continuità ICT**

Procedura Continuità operativa e continuità ICT

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-ACC-001 - Gestione accessi**

Procedura Gestione accessi

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-AST-001 - Gestione asset informativi**

Procedura Gestione asset informativi

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-SUP-001 - Gestione fornitori e terze parti**

Procedura Gestione fornitori e terze parti

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-INC-001 - Gestione incidenti di sicurezza**

Procedura Gestione incidenti di sicurezza

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.

**PROC-VUL-001 - Gestione vulnerabilità**

Procedura Gestione vulnerabilità

Scopo
Stabilire regole operative coerenti con il SGSI di DNS INFORMATICA S.A.S. di MARCO RACCA & C..

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.

Riferimenti al contesto

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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Server / infrastruttura virtuale: Diffusione malware / ransomware [Critico]
- Database clienti: Perdita o indisponibilità dei dati [Critico]
- Database clienti: Modifica non autorizzata dei dati [Alto]
- Database clienti: Violazione della confidenzialità delle informazioni [Alto]
- Database clienti: Errore umano nella gestione documenti o dati [Alto]
- Database clienti: Accesso non autorizzato ai dati [Alto]

- Asset: Smarrimento o furto di dispositivo [Medio]
- Asset: Interruzione servizio da fornitore SaaS / cloud [Medio]

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 (not_applicable)
- A.5.9 Inventario degli asset informativi (in_progress)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato
- 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 asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Trasferire: Trasferire o mitigare il rischio definendo SLA, misure contrattuali, requisiti di continuità del fornitore e soluzioni alternative. Controlli suggeriti: A.5.19 Information security in supplier relationships; A.5.23 Information security for use of cloud services. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile IT 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 Database clienti, con owner Direzione / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, 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.