SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Politica Sicurezza Informazioni

Nubys S.r.l. è una società italiana e start-up innovativa specializzata nell'analisi, progettazione, sviluppo, integrazione, manutenzione e commercializzazione di applicativi, piattaforme digitali e soluzioni software su misura ad alto contenuto tecnologico.

L'organizzazione supporta principalmente piccole e medie imprese e studi professionali nei processi di trasformazione digitale, sviluppando sistemi informatici scalabili finalizzati alla digitalizzazione, automazione e ottimizzazione dei processi aziendali. Le competenze di Nubys comprendono sviluppo web, integrazione di sistemi informativi, Robotic Process Automation, intelligenza artificiale, Microsoft Power Platform, Microsoft 365, gestione e analisi dei dati, assessment dei processi e consulenza tecnologica.

Nubys adotta un approccio strutturato che comprende analisi delle esigenze, definizione della strategia, progettazione, sviluppo, collaudo, rilascio, manutenzione e assistenza continuativa, con particolare attenzione alla sicurezza, all'affidabilità, alla scalabilità e all'integrazione delle soluzioni realizzate.

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

Nubys S.r.l. è una società italiana e start-up innovativa specializzata nell'analisi, progettazione, sviluppo, integrazione, manutenzione e commercializzazione di applicativi, piattaforme digitali e soluzioni software su misura ad alto contenuto tecnologico.

L'organizzazione supporta principalmente piccole e medie imprese e studi professionali nei processi di trasformazione digitale, sviluppando sistemi informatici scalabili finalizzati alla digitalizzazione, automazione e ottimizzazione dei processi aziendali. Le competenze di Nubys comprendono sviluppo web, integrazione di sistemi informativi, Robotic Process Automation, intelligenza artificiale, Microsoft Power Platform, Microsoft 365, gestione e analisi dei dati, assessment dei processi e consulenza tecnologica.

Nubys adotta un approccio strutturato che comprende analisi delle esigenze, definizione della strategia, progettazione, sviluppo, collaudo, rilascio, manutenzione e assistenza continuativa, con particolare attenzione alla sicurezza, all'affidabilità, alla scalabilità e all'integrazione delle soluzioni realizzate.

DESCRIZIONE DEL SERVIZIO

Il servizio comprende l’analisi dei processi e dei requisiti funzionali, tecnologici e di sicurezza del cliente, la progettazione, lo sviluppo, l’integrazione, il collaudo, il rilascio, la manutenzione e l’assistenza di applicativi, piattaforme digitali e sistemi software personalizzati.

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

assessment dei processi aziendali e dell’infrastruttura informatica;
raccolta, analisi e formalizzazione dei requisiti;
studi di fattibilità e analisi organizzative;
progettazione di architetture software scalabili;
sviluppo di applicativi, gestionali e portali web personalizzati;
progettazione di interfacce responsive e user experience;
integrazione con software gestionali, database, sistemi ERP e piattaforme esistenti;
integrazione mediante API e connettori applicativi;
sviluppo di soluzioni basate su Microsoft Power Platform;
configurazione e integrazione di Microsoft 365, Teams, SharePoint, OneDrive, Exchange e Azure;
automazione dei processi mediante RPA;
progettazione e integrazione di soluzioni di intelligenza artificiale;
gestione, elaborazione e analisi dei dati;
migrazione di dati e applicazioni;
configurazione di ruoli, profili e autorizzazioni;
definizione di policy di governance e Data Loss Prevention;
test funzionali, tecnici e di sicurezza;
rilascio e messa in esercizio delle soluzioni;
gestione delle modifiche, aggiornamenti e correzione degli errori;
manutenzione evolutiva, preventiva e correttiva;
supporto tecnico e assistenza post-progetto;
formazione e affiancamento degli utenti.

I servizi sono erogati attraverso un ciclo di sviluppo controllato e documentato, applicando criteri di sicurezza fin dalla progettazione e assicurando, in relazione ai requisiti concordati, la riservatezza, l’integrità, la disponibilità, l’autenticità e la tracciabilità delle informazioni.

Le responsabilità, i requisiti di sicurezza, i livelli di servizio, le modalità di rilascio, l’assistenza, la gestione delle modifiche e la protezione dei dati sono definiti negli accordi contrattuali e nella documentazione di progetto.

INDICE DEL DOCUMENTO

TERMINI IN USO

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

IMPEGNO DELLA DIREZIONE

La Direzione di NUBYS S.R.L. 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 Nubys S.r.l. si applica all'analisi, progettazione, sviluppo, configurazione, integrazione, collaudo, rilascio, manutenzione e assistenza di applicativi, piattaforme digitali e soluzioni software personalizzate finalizzate alla digitalizzazione, automazione e ottimizzazione dei processi aziendali.

Il perimetro comprende le attività di sviluppo software e web, analisi funzionale, progettazione UX/UI, consulenza tecnologica, assessment dei processi, integrazione di sistemi informativi, sviluppo mediante Microsoft Power Platform, configurazione e integrazione di Microsoft 365, automazione RPA, applicazione di tecnologie di intelligenza artificiale, gestione e analisi dei dati e assistenza post-rilascio. Nubys realizza soluzioni su misura, scalabili e integrabili con i sistemi già utilizzati dai clienti.

Sono compresi nello scopo i seguenti processi:

direzione, pianificazione strategica e governo del SGSI;
analisi del contesto e gestione dei rischi per la sicurezza delle informazioni;
gestione commerciale e valutazione delle richieste del cliente;
raccolta, analisi, validazione e gestione dei requisiti;
studio di fattibilità e analisi dei processi aziendali;
pianificazione e gestione dei progetti;
progettazione delle architetture software;
progettazione funzionale e UX/UI;
sviluppo, revisione, test e manutenzione del codice;
gestione dei repository e del versionamento;
gestione delle configurazioni, delle modifiche e dei rilasci;
sviluppo e integrazione mediante API, connettori e servizi cloud;
gestione degli ambienti di sviluppo, test, collaudo e produzione;
gestione delle vulnerabilità applicative e delle dipendenze software;
gestione degli accessi, delle identità e dei privilegi;
gestione degli incidenti di sicurezza;
backup, ripristino e continuità operativa;
gestione dei fornitori e dei servizi esterni;
assistenza tecnica, manutenzione e supporto post-progetto;
formazione e affiancamento degli utenti;
gestione documentale, contrattuale e amministrativa;
gestione delle competenze e della consapevolezza del personale;
audit interno, riesame della Direzione, non conformità e miglioramento continuo.

Il perimetro organizzativo comprende:

gli amministratori e l'Alta Direzione;
il Chief Technology Officer;
il Technical Project Manager;
gli sviluppatori software;
la funzione di analisi funzionale e UX/UI;
la funzione commerciale;
il personale amministrativo;
i collaboratori, consulenti e fornitori che accedono a dati, sistemi, codice sorgente o ambienti compresi nel SGSI.

La società risulta composta da quattro dipendenti e tre collaboratori. Le funzioni pubblicate comprendono direzione commerciale, direzione tecnica, gestione dei progetti, sviluppo software e analisi funzionale e UX/UI.

Il perimetro fisico comprende:

sede legale: Via Oslavia 17, 20134 Milano;
unità locale e ufficio operativo: Via Ticino 51, 28068 Romentino (NO);
postazioni di lavoro remoto formalmente autorizzate;
attività svolte presso le sedi dei clienti;
data center, ambienti cloud e infrastrutture di fornitori esterni limitatamente ai servizi sotto la responsabilità o il controllo di Nubys.

La sede di Milano è registrata per l'attività di programmazione informatica, mentre l'unità locale di Romentino è classificata come ufficio per servizi connessi alle tecnologie dell'informazione.

Sono comprese nello scopo le seguenti categorie di informazioni:

dati anagrafici, amministrativi e contrattuali dei clienti;
requisiti funzionali, tecnici e di sicurezza;
informazioni sui processi e sull'organizzazione dei clienti;
dati personali e dati aziendali trattati dalle applicazioni;
codice sorgente, script, componenti e librerie;
credenziali, chiavi, certificati, token e segreti applicativi;
architetture, configurazioni, diagrammi e documentazione tecnica;
prototipi, mock-up, specifiche e documentazione UX/UI;
database, dataset, modelli analitici e dati utilizzati da sistemi di intelligenza artificiale;
ticket, anomalie, richieste di modifica e registrazioni degli interventi;
log applicativi, audit trail e report di monitoraggio;
backup e informazioni necessarie al ripristino;
contratti, offerte, ordini e documentazione dei fornitori;
dati del personale e documentazione del SGSI;
proprietà intellettuale, know-how e software sviluppato da Nubys.

La società dispone inoltre di un programma per elaboratore registrato presso la SIAE, che costituisce un asset di proprietà intellettuale rilevante per il SGSI.

Il perimetro tecnologico comprende:

postazioni di lavoro e dispositivi mobili autorizzati;
reti e sistemi aziendali;
piattaforme di posta elettronica, collaborazione e condivisione;
Microsoft 365, Teams, SharePoint, OneDrive, Exchange e Azure, ove utilizzati;
Microsoft Power Platform, Power Apps, Power Automate e Power BI;
repository del codice sorgente e sistemi di versionamento;
strumenti di project management, ticketing e documentazione;
ambienti di sviluppo, test, staging e produzione;
pipeline di compilazione, test e rilascio;
database, API e servizi di integrazione;
sistemi di backup, monitoraggio e logging;
infrastrutture cloud direttamente gestite o fornite da terze parti;

ambienti dei clienti ai quali Nubys accede in forza di specifica autorizzazione contrattuale.

Sono escluse esclusivamente le infrastrutture e le attività sulle quali Nubys non esercita responsabilità, controllo o accesso autorizzato. Ogni esclusione deve essere motivata, documentata e approvata dall'Alta Direzione, verificando che non comprometta la riservatezza, l'integrità e la disponibilità delle informazioni.

OBIETTIVI

Nubys S.r.l. stabilisce i seguenti obiettivi per la sicurezza delle informazioni. Gli obiettivi sono monitorati periodicamente e riesaminati almeno annualmente dall'Alta Direzione.

Obiettivo	Indicatore	Traguardo
Proteggere gli account privilegiati	Account amministrativi e dei repository protetti mediante MFA	100%
Controllare gli accessi	Account e privilegi sottoposti a riesame formale	Almeno semestrale
Revocare tempestivamente gli accessi	Accessi revocati dopo cessazione o cambio di ruolo	Entro 1 giorno lavorativo
Proteggere i repository	Repository privati con autorizzazioni nominative e logging attivo	100%
Applicare lo sviluppo sicuro	Progetti soggetti a requisiti e checklist di sicurezza	100% dei nuovi progetti
Garantire la revisione del codice	Modifiche critiche sottoposte a peer review	100%
Verificare la sicurezza prima del rilascio	Rilasci critici sottoposti a test di sicurezza	100%
Gestire le vulnerabilità critiche	Vulnerabilità critiche corrette, mitigate o formalmente accettate	Entro 15 giorni
Gestire le vulnerabilità elevate	Vulnerabilità elevate corrette, mitigate o formalmente accettate	Entro 30 giorni
Controllare le dipendenze software	Progetti critici sottoposti a verifica periodica di librerie e componenti	100%
Proteggere chiavi e segreti	Credenziali e token esclusi dal codice sorgente e conservati in strumenti protetti	100%
Separare gli ambienti	Progetti critici con separazione tra sviluppo, test e produzione	100%
Garantire la tracciabilità dei rilasci	Rilasci collegati a versione, approvazione e registrazione delle modifiche	100%
Garantire l'efficacia dei backup	Backup critici completati con esito positivo	Almeno 98%
Verificare il ripristino	Test documentati di ripristino di codice, configurazioni e dati critici	Almeno trimestrale
Garantire la continuità operativa	Prova del piano di continuità o disaster recovery	Almeno annuale
Gestire gli incidenti	Incidenti registrati, classificati e assegnati	100%
Escalare gli incidenti critici	Incidenti critici comunicati al responsabile	Entro 1 ora dalla conferma
Analizzare le cause	Incidenti rilevanti sottoposti a root cause analysis	100%
Formare il personale	Personale che completa la formazione annuale sulla sicurezza	100%
Formare gli sviluppatori	Sviluppatori formati annualmente sul secure coding	100%
Migliorare la consapevolezza	Personale sottoposto a verifica o simulazione di phishing	Almeno annuale
Controllare i fornitori critici	Fornitori critici valutati sotto il profilo della sicurezza	100% ogni anno
Proteggere la proprietà intellettuale	Asset software e documentazione critica inventariati e assegnati a un responsabile	100%
Mantenere aggiornato il registro rischi	Riesame dei rischi e delle opportunità	Almeno trimestrale e dopo modifiche rilevanti
Verificare il SGSI	Audit interno completo	Almeno annuale
Garantire il governo del SGSI	Riesame dell'Alta Direzione	Almeno annuale
Gestire le non conformità	Non conformità con causa, responsabile, azione e scadenza	100%
Proteggere i dati dei clienti	Incidenti gravi causati dalla mancata applicazione di controlli approvati	Obiettivo: zero
Migliorare la soddisfazione dei clienti	Reclami relativi a sicurezza e indisponibilità analizzati e trattati	100%

Per ogni obiettivo l'Alta Direzione assegna un responsabile, definisce le risorse necessarie, la frequenza di misurazione, le fonti dei dati e le evidenze da conservare. Gli scostamenti rispetto ai traguardi 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	Contabilita, 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 continuita operativa.
Sicurezza delle informazioni	Coordinamento SGSI, verifica controlli, gestione miglioramenti e supporto alla conformita.
Commerciale	Gestione clienti, offerte, sviluppo commerciale e mantenimento relazioni.
Operations	Pianificazione operativa, assegnazione attivita, monitoraggio esecuzione e continuita operativa.
Qualita e Compliance	Gestione procedure, verifiche interne, conformita normativa e presidio documentale.

RIESAME

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