SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Manuale SGSI

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-MAN-001
Data documento	20/07/2026
Versione	00
Approvato da	Alta direzione

PRESENTAZIONE

Il presente documento è redatto per fornire una rappresentazione organica, elegante e professionale del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione, collegando business, asset, rischi, controlli, responsabilità e miglioramento continuo in un impianto coerente con la ISO/IEC 27001:2022.

SCOPO

Lo scopo del documento è supportare direzione, funzioni aziendali, auditor, consulenti e parti autorizzate nella comprensione del perimetro del SGSI, della logica di governo adottata, delle priorità di rischio e delle misure poste a presidio delle informazioni e dei servizi rilevanti.

DESCRIZIONE DELL'AZIENDA

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.

1. SCOPO E FINALITÀ DEL MANUALE

1.1 Scopo del manuale

Il presente Manuale SGSI definisce l’architettura di governo, i criteri metodologici, i ruoli, i processi e le regole operative mediante cui NUBYS S.R.L. istituisce, attua, mantiene e migliora il proprio Sistema di Gestione per la Sicurezza delle Informazioni. Il manuale costituisce il riferimento di alto livello del sistema e

raccorda contesto organizzativo, analisi dei rischi, piano di trattamento, controlli applicabili, procedure operative, riesame e miglioramento continuo, in coerenza con i requisiti della ISO/IEC 27001 e con le migliori pratiche internazionali di governance.

1.2 Profilo aziendale

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.

1.3 Campo di applicazione di alto livello

Il SGSI è concepito per proteggere informazioni, asset, processi e servizi che sostengono gli obiettivi aziendali, salvaguardando riservatezza, integrità, disponibilità, autenticità e tracciabilità dove necessario.

1.4 Politica per la sicurezza delle informazioni

La Direzione si impegna a garantire che la sicurezza delle informazioni sia allineata agli obiettivi di business, sostenuta da adeguate risorse, integrata nei processi aziendali e riesaminata periodicamente per assicurarne efficacia, pertinenza e miglioramento continuo.

2. CAMPO DI APPLICAZIONE DEL SGSI

Il Sistema di Gestione per la Sicurezza delle Informazioni di 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.

Il perimetro del SGSI comprende persone, processi, informazioni, tecnologie, servizi e siti inclusi nell'ambito dichiarato, nonché gli asset e i trattamenti correlati che possono influire su riservatezza, integrità e disponibilità delle informazioni rilevanti per l'organizzazione e per le parti interessate.

2.1 Confini fisici, logici e organizzativi

I confini del sistema includono le sedi, le unità organizzative, le piattaforme, le infrastrutture, i servizi e i flussi informativi ricompresi nel perimetro dichiarato. Sono inclusi anche i fornitori critici, i processi esternalizzati e gli ambienti digitali che trattano o supportano informazioni rilevanti per il business.

3. RIFERIMENTI NORMATIVI E CRITERI DI CONFORMITÀ

3.1 Riferimenti applicabili

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR / Regolamento (UE) 2016/679
- NIS2 ove applicabile
- Obblighi contrattuali e requisiti cliente
- Policy, procedure e registrazioni interne del SGSI

3.2 Criteri di conformità

Il sistema è sviluppato assumendo come quadro di riferimento la ISO/IEC 27001, la Statement of Applicability aziendale, le procedure interne, gli obblighi contrattuali, i requisiti cogenti applicabili e gli impegni assunti verso clienti, partner, personale, fornitori e altre parti interessate. Eventuali requisiti aggiuntivi di natura legale, regolatoria, settoriale o contrattuale devono essere recepiti nei registri, nei controlli e nei piani di azione del SGSI.

4. CONTESTO DELL’ORGANIZZAZIONE E PARTI INTERESSATE

4.1 Analisi del contesto interno

Nubys S.r.l. è una start-up innovativa con una struttura organizzativa snella e specializzata nello sviluppo di soluzioni software personalizzate ad alto valore tecnologico. L’organizzazione è guidata da due amministratori, Giancarlo Martinelli e Marco Racca, mentre la responsabilità tecnica e il coordinamento delle attività tecnologiche sono attribuiti al Chief Technology Officer Jasson Campaña Moral.

Le attività sono svolte da un gruppo multidisciplinare che comprende direzione commerciale, direzione tecnica, gestione dei progetti, sviluppo software, analisi funzionale e progettazione UX/UI.

I principali fattori interni rilevanti per il SGSI sono:

dimensione contenuta dell’organizzazione e possibile concentrazione di più responsabilità sulle medesime persone;
presenza di due amministratori con poteri di gestione e rappresentanza;
ruolo centrale del CTO nella progettazione, nello sviluppo e nel coordinamento tecnico;
dipendenza dalle competenze specialistiche del personale;
necessità di garantire sostituzione e continuità in caso di indisponibilità di risorse chiave;
utilizzo di modalità di lavoro flessibili e postazioni remote;
gestione contemporanea di più progetti e clienti;
trattamento di codice sorgente, credenziali, dati dei clienti e proprietà intellettuale;
necessità di formalizzare ruoli, deleghe, autorizzazioni e responsabilità;
necessità di separare, ove possibile, sviluppo, approvazione, test e rilascio;
utilizzo di piattaforme cloud, strumenti collaborativi e repository esterni;
dipendenza da Microsoft 365, Power Platform, Azure e ulteriori servizi tecnologici;
necessità di mantenere aggiornati inventari, repository, librerie e dipendenze software;
necessità di controllare accessi privilegiati, token, API key e segreti applicativi;
esigenza di integrare sicurezza e privacy fin dalla progettazione;
necessità di proteggere gli ambienti di sviluppo, test e produzione;
esigenza di garantire revisione del codice, test e tracciabilità delle modifiche;
dipendenza dalla disponibilità delle connessioni e dei servizi cloud;
necessità di gestire conoscenze, documentazione e trasferimento delle competenze;
necessità di mantenere una formazione continua su tecnologie, sicurezza e sviluppo sicuro;
protezione del software e del know-how aziendale;
necessità di assicurare tempestiva assistenza e manutenzione dopo il rilascio.

Tra i punti di forza interni si considerano la specializzazione nello sviluppo su misura, la presenza di competenze tecniche differenziate, l’integrazione tra analisi funzionale e sviluppo, la capacità di accompagnare il cliente dal prototipo alla soluzione e l’erogazione di manutenzione e aggiornamenti successivi alla consegna.

Nell’analisi del contesto è inoltre valutata l’eventuale rilevanza del cambiamento climatico rispetto alla disponibilità delle sedi, delle connessioni, dei servizi cloud e delle infrastrutture dei fornitori, in coerenza con l’Amendment 1:2024 applicabile alla ISO/IEC 27001:2022.

4.2 Analisi del contesto esterno

Nubys opera in un mercato caratterizzato dalla rapida evoluzione delle tecnologie digitali, dalla crescente domanda di automazione e dalla necessità delle organizzazioni clienti di integrare applicazioni, dati e piattaforme cloud.

I principali fattori esterni rilevanti sono:

aumento della domanda di software personalizzato e automazione dei processi;
rapida evoluzione di Microsoft 365, Power Platform, Azure, RPA e intelligenza artificiale;
frequenti aggiornamenti di linguaggi, framework, librerie, API e servizi cloud;
rischio di obsolescenza delle tecnologie e delle competenze;
aumento di ransomware, phishing, furto di credenziali e compromissione degli account;
vulnerabilità nelle librerie open source e negli elementi della catena di fornitura software;
attacchi ai repository, alle pipeline di sviluppo e agli ambienti cloud;
rischio di esposizione accidentale di codice sorgente, token, API key e dati dei clienti;
dipendenza da Microsoft e da altri fornitori di servizi cloud, hosting, software e collaborazione;
indisponibilità, modifica o cessazione di servizi forniti da terze parti;
requisiti contrattuali relativi a riservatezza, livelli di servizio, proprietà del codice, manutenzione e continuità;
obblighi applicabili in materia di protezione dei dati personali, proprietà intellettuale, licenze software, rapporti di lavoro e conservazione documentale;
richieste dei clienti relative a privacy e security by design;
necessità di disciplinare il trattamento dei dati utilizzati in sistemi di intelligenza artificiale;
aspettative dei clienti riguardo a sicurezza, affidabilità, scalabilità e integrazione;
concorrenza di software house, società di consulenza e piattaforme low-code;
difficoltà di reperimento e mantenimento di sviluppatori qualificati;
aspettative di assistenza continuativa e rapida correzione delle anomalie;
rischi connessi a interruzioni di energia, connettività e data center;
possibili eventi climatici o ambientali che interessino sedi e infrastrutture esterne;
evoluzione degli obblighi normativi e degli standard relativi alla cybersecurity e all’intelligenza artificiale.

I clienti di riferimento comprendono principalmente PMI e studi professionali che richiedono soluzioni digitali personalizzate, integrazione con sistemi esistenti e assistenza continuativa.

4.3 Parti interessate e relative esigenze

Alta Direzione e soci

Si aspettano:

protezione della proprietà intellettuale e del valore aziendale;
continuità economica e operativa;
controllo dei rischi;
tutela della reputazione;
rispetto degli obblighi applicabili;
disponibilità di informazioni attendibili per le decisioni;
crescita sostenibile dell’organizzazione.
Dipendenti e collaboratori

Si aspettano:

ruoli, responsabilità e autorizzazioni chiari;
strumenti affidabili e sicuri;
accessi adeguati alle attività assegnate;
formazione e aggiornamento professionale;
protezione dei dati personali;
disponibilità della documentazione;
continuità delle attività e supporto in caso di incidente.

Clienti e relativi utenti

Si aspettano:

riservatezza delle informazioni condivise;
integrità e affidabilità del software;
disponibilità delle applicazioni e dei servizi;
rispetto dei requisiti funzionali e di sicurezza;
protezione dei dati personali e aziendali;
tracciabilità delle modifiche;
rispetto delle scadenze e dei livelli di servizio;
tempestiva gestione delle anomalie;
manutenzione e aggiornamento delle soluzioni;
comunicazione trasparente in caso di incidente.
Amministratori dei sistemi dei clienti

Si aspettano:

integrazioni controllate e documentate;
API sicure;
account nominativi e privilegi limitati;
configurazioni affidabili;
documentazione tecnica aggiornata;
collaborazione nella gestione degli incidenti e delle modifiche.
Utenti delle applicazioni

Si aspettano:

disponibilità e facilità di utilizzo;
protezione dei propri dati;
autenticazione e autorizzazione adeguate;
correttezza delle funzionalità;
assistenza e formazione.
Fornitori cloud e tecnologici

Si aspettano:

rispetto delle condizioni contrattuali e di licenza;
utilizzo corretto dei servizi;
protezione degli account;
gestione sicura delle integrazioni;
collaborazione in caso di incidente o vulnerabilità.
Sviluppatori e comunità open source

Si aspettano il rispetto delle licenze, delle attribuzioni e delle condizioni d’uso dei componenti incorporati nelle soluzioni.

Partner e subfornitori

Si aspettano:

responsabilità definite;
autorizzazioni formalizzate;
accessi limitati alle necessità operative;
protezione delle informazioni ricevute;
rispetto degli accordi di riservatezza;
modalità chiare di collaborazione e comunicazione.
Autorità e organismi di controllo

Si aspettano:

rispetto delle disposizioni applicabili;
disponibilità di registrazioni ed evidenze;
collaborazione durante verifiche e accertamenti;
corretta gestione delle eventuali comunicazioni obbligatorie.
Interessati al trattamento dei dati personali

Si aspettano liceità, correttezza e trasparenza, protezione dei dati, limitazione degli accessi, rispetto dei tempi di conservazione e gestione dei diritti riconosciuti dalla normativa. Il sito Nubys dichiara il trattamento di dati relativi a utenti e contatti e l'utilizzo di servizi esterni e piattaforme di hosting.

Organismo di certificazione e auditor

Si aspettano:

evidenze oggettive di applicazione del SGSI;
disponibilità della documentazione;
tracciabilità delle decisioni;
indipendenza delle verifiche;
gestione delle non conformità;
impegno al miglioramento continuo.
Comunità e territorio

Si aspettano comportamento responsabile, continuità dell'attività, corretta gestione delle tecnologie e attenzione agli impatti energetici e ambientali dei servizi digitali.

L'organizzazione valuta periodicamente le evoluzioni del contesto e le aspettative delle parti interessate, verificandone l'impatto sul perimetro, sui rischi, sui controlli e sulla documentazione del sistema.

5. LEADERSHIP, GOVERNO E RESPONSABILITÀ

5.1 Ruoli, responsabilità e autorità

La Direzione assicura indirizzo strategico, disponibilità delle risorse, integrazione del SGSI nei processi aziendali, approvazione delle politiche e riesame periodico delle prestazioni del sistema. I responsabili di funzione e gli owner degli asset presidiano i rischi di competenza, sostengono l'attuazione dei controlli, promuovono la consapevolezza del personale e garantiscono la gestione delle evidenze documentate. Tutto il personale e i collaboratori sono tenuti ad operare secondo ruoli, autorizzazioni e responsabilità formalmente assegnate.

5.2 Funzioni aziendali censite

Funzione	Scopo	Responsabilità	Attività
Direzione	Definire indirizzi, priorita e supervisione generale dell'organizzazione.	Governance aziendale, approvazione decisioni, riesame obiettivi e supervisione del sistema di gestione.	Pianificazione strategica, approvazioni, coordinamento dei responsabili, monitoraggio risultati.
Amministrazione	Gestire aspetti amministrativi, contabili e documentali dell'organizzazione.	Contabilita, scadenze amministrative, gestione documentazione economico-amministrativa.	Registrazioni contabili, gestione pagamenti, archiviazione documenti amministrativi.
Risorse Umane	Gestire personale, ruoli, inserimenti e aspetti organizzativi connessi alle persone.	Anagrafica personale, onboarding, gestione ruoli e coordinamento esigenze formative.	Aggiornamento organigramma, raccolta dati personale, gestione comunicazioni HR.
IT	Supportare sistemi informativi, strumenti digitali e continuita operativa tecnologica.	Gestione infrastruttura IT, supporto utenti, sicurezza tecnica di base e continuita operativa.	Assistenza tecnica, gestione account, backup, presidio dei sistemi e delle dotazioni informatiche.
Sicurezza delle informazioni	Presidiare aspetti organizzativi e operativi relativi alla sicurezza delle informazioni.	Coordinamento SGSI, verifica controlli, gestione miglioramenti e supporto alla conformita.	Analisi rischi, aggiornamento controlli, supporto SoA, monitoraggio azioni di trattamento.
Commerciale	Gestire relazioni commerciali, clienti, offerte e sviluppo opportunita.	Gestione clienti, offerte, sviluppo commerciale e mantenimento relazioni.	Contatti commerciali, preventivi, aggiornamento opportunita e coordinamento richieste clienti.
Operations	Coordinare l'operativita corrente e l'erogazione dei servizi o delle attivita principali.	Pianificazione operativa, assegnazione attivita, monitoraggio esecuzione e continuita operativa.	Coordinamento operativo, pianificazione attivita, controllo

Funzione	Scopo	Responsabilità	Attività
			avanzamento e gestione priorita.
Qualita e Compliance	Supportare conformita, procedure, controlli documentali e miglioramento continuo.	Gestione procedure, verifiche interne, conformita normativa e presidio documentale.	Aggiornamento documenti, raccolta evidenze, verifica attuazione procedure e supporto audit.

5.3 Persone e ruoli censiti

Nominativo	Ruolo	Funzione	Responsabile diretto	Stato
Adele Gropplero di Troppenburg	Junior Software Developer	Operations	Giancarlo Martinelli	Attivo
Eugenio Peressi	Senior Software Developer	Operations	Giancarlo Martinelli	Attivo
Francesca Fornari	Functional Analyst & UX/UI Designer	Qualita e Compliance		Attivo
Giancarlo Martinelli	Amministratore	Amministrazione		Attivo
Jasson Steven Campaña Moral	Chief Technology Officer	IT	Giancarlo Martinelli	Attivo
Marco Racca	Founder – Sales Manager.	Commerciale		Attivo
Mikhael Ponticiello	Technical Project Manager	Operations	Giancarlo Martinelli	Attivo
Nadir Yousif	Software Developer	Operations		Attivo

5.4 Risorse e competenze

Le risorse necessarie in termini di persone, competenze, tecnologie, budget e supporto operativo sono pianificate in modo coerente con priorità di rischio, obblighi di conformità e obiettivi del business.

5.5 Comunicazione

I flussi informativi interni ed esterni relativi al SGSI sono stabiliti per garantire tempestività, tracciabilità, adeguata autorizzazione e corretta gestione delle evidenze documentate.

6. SEDI, UNITÀ ORGANIZZATIVE E AMBIENTI INCLUSI

Sito	Indirizzo	Paese	Note
Sede legale	Via Oslavia 17 Milano	Italia	Sede di programmazione informatica
Unità locale – Ufficio operativo	Via Ticino 51 Romentino	Italia	infrastrutture cloud e piattaforme utilizzate per sviluppo, collaudo, rilascio e assistenza; repository del codice sorgente e ambienti di collaborazione; postazioni di lavoro remoto formalmente autorizzate; ambienti informatici dei clienti ai quali Nubys accede per attività contrattualmente autorizzate.

Numero siti/ambienti censiti nel perimetro: **2**.

7. ASSET INFORMATIVI E CRITERI DI CLASSIFICAZIONE

Gli asset del SGSI comprendono informazioni, servizi, applicazioni, infrastrutture, dispositivi, archivi documentali, risorse umane, sedi e altri elementi di supporto al business. Ciascun asset deve essere identificato, associato a un owner, classificato secondo i requisiti di riservatezza, integrità e disponibilità e gestito lungo il relativo ciclo di vita.

7.1 Criteri di classificazione

La classificazione degli asset e delle informazioni considera criticità per il business, requisiti contrattuali, impatti legali/regolatori e conseguenze operative in caso di compromissione o indisponibilità.

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

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

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

8. METODOLOGIA DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO

8.1 Metodologia di valutazione dei rischi

L'organizzazione adotta una metodologia strutturata di risk assessment e risk treatment che prende in considerazione contesto, asset, minacce, vulnerabilità, probabilità, impatto e livello di rischio risultante. I criteri di accettazione del rischio, le priorità di intervento e le decisioni di trattamento sono definiti in modo coerente con gli obiettivi di business, la propensione al rischio dell'organizzazione, gli obblighi applicabili e le capacità operative disponibili.

8.2 Opzioni di trattamento

Le opzioni di trattamento includono riduzione, trasferimento, evitamento o accettazione motivata del rischio. La metodologia viene aggiornata quando intervengono cambiamenti rilevanti nel contesto, nel perimetro, nelle tecnologie, nei processi, nei requisiti contrattuali o nel panorama delle minacce.

9. QUADRO DEI RISCHI E PRIORITÀ DI INTERVENTO

9.1 Report di valutazione del rischio

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
Server / infrastruttura virtuale	Diffusione malware / ransomware	Sistemi non aggiornati o protezioni endpoint insufficienti	15	Critico	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities.
Database clienti	Perdita o indisponibilità dei dati	Backup assenti o non verificati	15	Critico	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity.
Database clienti	Modifica non autorizzata dei dati	Permessi eccessivi o assenza di tracciamento log	12	Alto	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights.
Database clienti	Violazione della confidenzialità delle informazioni	Classificazione dati assente o canali di invio non protetti	12	Alto	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.
Database clienti	Errore umano nella gestione documenti o dati	Procedure non formalizzate o formazione insufficiente	12	Alto	Mitigare il rischio formalizzando istruzioni operative, verifiche a campione e formazione periodica al personale. Controlli suggeriti: A.6.3 Information security awareness, education and training; A.5.10 Acceptable use of information and other associated assets.
Database clienti	Accesso non autorizzato ai	Password deboli o	12	Alto	Mitigare il rischio applicando il principio del minimo privilegio,

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
	dati	mancata MFA			attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights.

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

10. OBIETTIVI SGSI, PIANIFICAZIONE E RISORSE

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.

Gli obiettivi del SGSI devono essere misurabili ove possibile, coerenti con la politica per la sicurezza delle informazioni, assegnati a responsabili identificati, monitorati tramite indicatori e riesaminati periodicamente. L'organizzazione garantisce risorse adeguate in termini di persone, competenze, tecnologie, budget, tempo e supporto operativo per l'attuazione delle iniziative di sicurezza.

11. CONTROLLI, STATEMENT OF APPLICABILITY E PIANO DI TRATTAMENTO

11.1 Controlli e SoA

I controlli del SGSI sono determinati in funzione dei risultati dell'analisi del rischio, dei requisiti applicabili e delle esigenze operative dell'organizzazione. La Statement of Applicability formalizza per ciascun controllo la decisione di applicabilità, lo stato di implementazione e la relativa motivazione.

11.2 Piano di trattamento del rischio

Il piano di trattamento traduce i rischi significativi in azioni, responsabilità, scadenze e stati di avanzamento, mantenendo coerenza tra rischio, controllo, responsabili e capacità attuativa del business.

Controlli applicabili o da confermare presenti in archivio: **28**. Azioni/piani di trattamento presenti: **8**. Procedure SGSI registrate: **8**.

12. COMPETENZA, CONSAPEVOLEZZA, COMUNICAZIONE E CONTROLLO DOCUMENTALE

12.1 Competenze e consapevolezza

L'organizzazione assicura che il personale operi con adeguata competenza e consapevolezza rispetto a ruoli, responsabilità, politiche, procedure e requisiti di sicurezza.

12.2 Controllo documentale

Le informazioni documentate del SGSI sono identificate, approvate, aggiornate, protette, rese disponibili e conservate in modo controllato per garantirne integrità, reperibilità e adeguatezza d'uso. Le comunicazioni interne ed esterne rilevanti per il SGSI sono pianificate, tracciate quando necessario e gestite secondo criteri di riservatezza e autorizzazione.

13. GESTIONE OPERATIVA, MONITORAGGIO E RISPOSTA AGLI EVENTI

13.1 Attuazione operativa

Le attività operative del SGSI comprendono l'attuazione dei controlli, la gestione dei cambiamenti, il monitoraggio delle misure di sicurezza, il presidio delle vulnerabilità, la gestione degli incidenti e la conservazione delle evidenze.

13.2 Risposta agli eventi e non conformità

Eventi, anomalie, non conformità e incidenti informativi devono essere rilevati, registrati, valutati, trattati e, ove opportuno, analizzati per identificarne cause, impatti e azioni correttive.

14. AUDIT INTERNI, RIESAME DELLA DIREZIONE E MIGLIORAMENTO CONTINUO

14.1 Audit e riesame

Il SGSI è sottoposto a audit interni pianificati, riesami periodici della Direzione e verifiche dell'efficacia delle misure adottate.

14.2 Miglioramento continuo

I risultati di audit, monitoraggi, incidenti, analisi dei rischi, trattamenti, indicatori e feedback delle parti interessate alimentano il processo di miglioramento continuo. Le azioni correttive e di miglioramento devono essere proporzionate ai rilievi emersi, assegnate a responsabili identificati e verificate fino alla loro chiusura.

15. ALLEGATI E DOCUMENTI CORRELATI

Il presente manuale si integra con il registro degli asset, il registro dei rischi, il piano di trattamento del rischio, la Statement of Applicability, la politica per la sicurezza delle informazioni, le procedure operative e ogni altra informazione documentata del SGSI rilevante ai fini del governo, della conformità e dell’efficacia del sistema.