SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Gestione accessi

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	PROC-ACC-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.

PROC-ACC-001 - GESTIONE ACCESSI

Procedura Gestione accessi

Scopo
Stabilire regole operative coerenti con il SGSI di NUBYS S.R.L..

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.

Riferimenti al contesto
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.

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 (implemented)

- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (not_applicable)
- A.5.9 Inventario degli asset informativi (implemented)
- 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.
- Accettare: 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.