SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Piano di Trattamento del Rischio

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-TRT-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.

PIANO DI TRATTAMENTO DEL RISCHIO

Rischio	Controllo	Tipo	Azione	Responsabile	Funzione	Persona	Scadenza	Stato
Smarrimento o furto di dispositivo / Cifratura assente e mancata gestione dispositivi mobili	A.5.24 Pianificazione della gestione incidenti	mitigate	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.	Responsabile IT	Amministrazione	Giancarlo Martinelli	2026-09-18	planned
Interruzione servizio da fornitore SaaS / cloud / Mancanza di SLA o di soluzioni alternative	A.5.19 Sicurezza delle informazioni nei rapporti con i fornitori	accept	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.	Responsabile IT	Amministrazione	Giancarlo Martinelli	2026-09-18	planned
Modifica non autorizzata dei dati / Permessi eccessivi o assenza di tracciamento log	A.5.15 Controllo degli accessi	mitigate	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	Responsabile IT	IT	Giancarlo Martinelli	2026-08-19	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Funzione	Persona	Scadenza	Stato
			organizzativi e tecnici proporzionati.					
Violazione della confidenzialità delle informazioni / Classificazione dati assente o canali di invio non protetti		mitigate	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.	Direzione / IT	IT	Eugenio Peressi	2026-08-19	planned
Errore umano nella gestione documenti o dati / Procedure non formalizzate o formazione insufficiente	A.5.1 Politiche per la sicurezza delle informazioni	mitigate	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.	Responsabile di processo	Sicurezza delle informazioni	Giancarlo Martinelli	2026-08-19	planned
Accesso non autorizzato ai dati / Password deboli o mancata MFA	A.5.18 Diritti di accesso	mitigate	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.	Responsabile IT	IT	Giancarlo Martinelli	2026-08-19	planned
Diffusione malware / ransomware / Sistemi non aggiornati o protezioni endpoint insufficienti	A.6.3 Consapevolezza e formazione	mitigate	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. Azione operativa suggerita: definire attività, evidenze,	Responsabile IT	Direzione	Giancarlo Martinelli	2026-08-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Funzione	Persona	Scadenza	Stato
			verifiche e responsabilità per Server / infrastruttura virtuale, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.					
Perdita o indisponibilità dei dati / Backup assenti o non verificati	A.5.1 Politiche per la sicurezza delle informazioni	mitigate	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. 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.	Responsabile IT	IT	Eugenio Peressi	2026-08-04	planned