SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Statement of Applicability

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-SOA-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

Dichiarazione di Applicabilità

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.

DICHIARAZIONE DI APPLICABILITÀ

La seguente tabella riporta i controlli considerati nel perimetro SGSI, l'applicabilità, lo stato di implementazione e la relativa giustificazione.

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
A.5.1	Politiche per la sicurezza delle informazioni	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.1 - Politiche per la sicurezza delle informazioni risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.2	Ruoli e responsabilità per la sicurezza delle informazioni	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.2 - Ruoli e responsabilità per la sicurezza delle informazioni risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.7	Threat intelligence	Organizzativi	No	not_applicable			Controllo non applicabile nel perimetro SGSI attuale. La

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							valutazione organizzativa ha escluso A.5.7 - Threat intelligence in funzione di contesto, asset, rischi e trattamenti attualmente censiti.
A.5.9	Inventario degli asset informativi	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.9 - Inventario degli asset informativi risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.10	Uso accettabile degli asset	Organizzativi	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.5.10 - Uso accettabile degli asset risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.12	Classificazione delle informazioni	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.12 - Classificazione delle informazioni risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.15	Controllo degli accessi	Organizzativi	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.5.15 - Controllo degli accessi risulta attuato nel SGSI aziendale con misure operative già adottate e

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							coerenti con il rischio valutato.
A.5.18	Diritti di accesso	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.18 - Diritti di accesso risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.19	Sicurezza delle informazioni nei rapporti con i fornitori	Organizzativi	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.5.19 - Sicurezza delle informazioni nei rapporti con i fornitori risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.23	Sicurezza per l'uso dei servizi cloud	Organizzativi	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.5.23 - Sicurezza per l'uso dei servizi cloud risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.5.24	Pianificazione della gestione incidenti	Organizzativi	Sì	in_progress	IT	Jasson Steven Campaña Moral	Controllo applicabile e in corso di implementazione. A.5.24 - Pianificazione della gestione incidenti è stato avviato e risulta oggetto di adeguamento nel piano SGSI.
A.5.29	Sicurezza durante la disruption	Organizzativi	Sì	in_progress	Operations	Adele Gropplero di Troppenburg	Controllo applicabile e in corso di implementazione. A.5.29 - Sicurezza

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							durante la disruption è stato avviato e risulta oggetto di adeguamento nel piano SGSI.
A.5.30	ICT readiness per la continuità	Organizzativi	Sì	planned	Operations	Eugenio Peressi	Controllo proposto automaticamente dal sistema sulla base del rischio: Perdita o indisponibilità dei dati. Vulnerabilità associata: Backup assenti o non verificati.
A.6.3	Consapevolezza e formazione	Persone	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.6.3 - Consapevolezza e formazione risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.6.5	Responsabilità a fine rapporto o cambio ruolo	Persone	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.6.5 - Responsabilità a fine rapporto o cambio ruolo risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.7.1	Perimetri di sicurezza fisica	Fisici	Sì	implemented	Operations	Nadir Yousif	Controllo applicabile e implementato. A.7.1 - Perimetri di sicurezza fisica risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.7.2	Controlli di accesso fisico	Fisici	Sì	implemented	Operations	Mikhael Ponticiello	Controllo applicabile e

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							implementato. A.7.2 - Controlli di accesso fisico risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.7.4	Monitoraggio sicurezza fisica	Fisici	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.7.4 - Monitoraggio sicurezza fisica risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.7.8	Collocazione e protezione apparecchiature	Fisici	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.7.8 - Collocazione e protezione apparecchiature risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.1	Dispositivi endpoint utente	Tecnologici	Sì	in_progress	IT	Jasson Steven Campaña Moral	Controllo applicabile e in corso di implementazione. A.8.1 - Dispositivi endpoint utente è stato avviato e risulta oggetto di adeguamento nel piano SGSI.
A.8.2	Accessi privilegiati	Tecnologici	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.8.2 - Accessi privilegiati risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
A.8.3	Restrizione accessi alle informazioni	Tecnologici	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.8.3 - Restrizione accessi alle informazioni risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.5	Autenticazione sicura	Tecnologici	Sì	in_progress	IT	Jasson Steven Campaña Moral	Controllo applicabile e in corso di implementazione. A.8.5 - Autenticazione sicura è stato avviato e risulta oggetto di adeguamento nel piano SGSI.
A.8.8	Gestione vulnerabilità tecniche	Tecnologici	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.8.8 - Gestione vulnerabilità tecniche risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.9	Configuration management	Tecnologici	Sì	planned	Amministrazione	Giancarlo Martinelli	Controllo proposto automaticamente dal sistema sulla base del rischio: Diffusione malware / ransomware. Vulnerabilità associata: Sistemi non aggiornati o protezioni endpoint insufficienti.
A.8.10	Cancellazione delle informazioni	Tecnologici	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e implementato. A.8.10 - Cancellazione delle informazioni risulta attuato nel

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.11	Data masking	Tecnologici	No	not_applicable			Controllo non applicabile nel perimetro SGSI attuale. La valutazione organizzativa ha escluso A.8.11 - Data masking in funzione di contesto, asset, rischi e trattamenti attualmente censiti.
A.8.12	Data leakage prevention	Tecnologici	No	not_applicable			Controllo non applicabile nel perimetro SGSI attuale. La valutazione organizzativa ha escluso A.8.12 - Data leakage prevention in funzione di contesto, asset, rischi e trattamenti attualmente censiti.
A.8.13	Backup delle informazioni	Tecnologici	Sì	implemented	IT	Jasson Steven Campaña Moral	Controllo applicabile e implementato. A.8.13 - Backup delle informazioni risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.15	Logging	Tecnologici	Sì	in_progress	IT	Jasson Steven Campaña Moral	Controllo applicabile e in corso di implementazione. A.8.15 - Logging è stato avviato e risulta oggetto di adeguamento nel piano SGSI.
A.8.16	Monitoring activities	Tecnologici	Sì	implemented	Amministrazione	Giancarlo Martinelli	Controllo applicabile e

Codice	Controllo	Dominio	Applicabile	Stato	Funzione	Persona	Giustificazione
							implementato. A.8.16 - Monitoring activities risulta attuato nel SGSI aziendale con misure operative già adottate e coerenti con il rischio valutato.
A.8.23	Web filtering	Tecnologici	No	not_applicable			Controllo non applicabile nel perimetro SGSI attuale. La valutazione organizzativa ha escluso A.8.23 - Web filtering in funzione di contesto, asset, rischi e trattamenti attualmente censiti.
A.8.24	Uso della crittografia	Tecnologici	No	not_applicable			Controllo non applicabile nel perimetro SGSI attuale. La valutazione organizzativa ha escluso A.8.24 - Uso della crittografia in funzione di contesto, asset, rischi e trattamenti attualmente censiti.