SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Piano di Trattamento del Rischio

GMK Sistemi S.r.l. è una società italiana specializzata nella consulenza, progettazione, implementazione e gestione di soluzioni IT e ICT rivolte principalmente a piccole e medie imprese e studi professionali. L'azienda opera come partner tecnologico unico, adottando un approccio consulenziale, proattivo e orientato alla continuità operativa, alla sicurezza delle informazioni e all'efficienza dei processi aziendali.
Le competenze di GMK Sistemi comprendono infrastrutture hardware e software, reti cablate e wireless, servizi cloud, cybersecurity, outsourcing IT, comunicazione unificata, noleggio operativo di tecnologie e automazione dei processi. L'organizzazione assicura supporto tecnico remoto e presso le sedi dei clienti, monitoraggio continuo, aggiornamento tecnologico e soluzioni personalizzate sulla base dei rischi, dei requisiti operativi e degli obiettivi del cliente

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

GMK Sistemi S.r.l. è una società italiana specializzata nella consulenza, progettazione, implementazione e gestione di soluzioni IT e ICT rivolte principalmente a piccole e medie imprese e studi professionali. L'azienda opera come partner tecnologico unico, adottando un approccio consulenziale, proattivo e orientato alla continuità operativa, alla sicurezza delle informazioni e all'efficienza dei processi aziendali.
Le competenze di GMK Sistemi comprendono infrastrutture hardware e software, reti cablate e wireless, servizi cloud, cybersecurity, outsourcing IT, comunicazione unificata, noleggio operativo di tecnologie e automazione dei processi. L'organizzazione assicura supporto tecnico remoto e presso le sedi dei clienti, monitoraggio continuo, aggiornamento tecnologico e soluzioni personalizzate sulla base dei rischi, dei requisiti operativi e degli obiettivi del cliente

DESCRIZIONE DEL SERVIZIO

Il servizio comprende l'analisi dei requisiti e dei rischi, la progettazione, la configurazione, l'implementazione, la gestione, la manutenzione, il monitoraggio e l'assistenza delle infrastrutture IT e ICT dei clienti.

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

gestione di server, postazioni di lavoro, dispositivi, reti e ambienti cloud;
assistenza tecnica, help desk e interventi da remoto e on-site;
monitoraggio proattivo delle infrastrutture e gestione degli eventi;
patch management e aggiornamento dei sistemi;
protezione degli endpoint mediante antivirus, EDR e XDR;
gestione di firewall UTM e sistemi di sicurezza perimetrale;
protezione della posta elettronica e prevenzione di spam, malware e phishing;
backup dei dati, backup degli ambienti Microsoft 365 e Google Workspace, ripristino e disaster recovery;
Data Loss Prevention e controllo degli accessi ai file;
networking, segmentazione delle reti e gestione degli apparati;
unified communication e sistemi VoIP;
noleggio operativo e gestione del ciclo di vita dell'hardware;
automazione dei processi aziendali mediante soluzioni software e RPA.

I servizi sono erogati applicando criteri di riservatezza, integrità, disponibilità, autenticità, tracciabilità e continuità operativa delle informazioni, con responsabilità, livelli di servizio, modalità di assistenza ed escalation definiti nei relativi contratti e accordi con i clienti.

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.5.1 Politiche per la sicurezza delle informazioni	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	Direzione	Giancarlo Martinelli	2026-09-18	planned
Interruzione servizio da fornitore SaaS / cloud / Mancanza di SLA o di soluzioni alternative	A.5.23 Sicurezza per l'uso dei servizi cloud	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	IT	Giancarlo Martinelli	2026-09-18	planned
Modifica non autorizzata dei dati / Permessi eccessivi o assenza di tracciamento log	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	Sicurezza delle informazioni	Giancarlo Martinelli	2026-08-19	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Funzione	Persona	Scadenza	Stato
			Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.					
Violazione della confidenzialità delle informazioni / Classificazione dati assente o canali di invio non protetti	A.5.24 Pianificazione della gestione incidenti	avoid	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	Direzione	Giancarlo Martinelli	2026-08-19	planned
Errore umano nella gestione documenti o dati / Procedure non formalizzate o formazione insufficiente	A.5.24 Pianificazione della gestione incidenti	accept	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	Direzione	Alessio Scattareggia	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	Davide Vegetti	2026-08-19	planned
Diffusione malware / ransomware / Sistemi non aggiornati o protezioni endpoint insufficienti	A.5.1 Politiche per la sicurezza delle informazioni	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	Responsabile IT	IT	Giancarlo Martinelli	2026-08-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Funzione	Persona	Scadenza	Stato
			Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, 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.5.12 Classificazione 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	Sicurezza delle informazioni	Alessio Scattareggia	2026-08-04	planned