SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Registro dei Rischi

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-RSK-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.

REGISTRO DEI RISCHI

Asset	Minaccia	Vulnerabilità	Impatto	Probabilità	Score	Livello	Responsabile	Funzione	Persona	Trattamento
Server / infrastruttura virtuale	Diffusione malware / ransomware	Sistemi non aggiornati o protezioni endpoint insufficienti	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT			Mitigare il rischio cor management, protez endpoint, filtro e-mai monitoraggio central degli eventi di sicure Controlli suggeriti: A. Management of tech vulnerabilities; A.8.9 Configuration manag A.8.16 Monitoring ac
Database clienti	Perdita o indisponibilità dei dati	Backup assenti o non verificati	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT			Mitigare il rischio implementando back periodici, test di ripris retention definita e monitoraggio dell'esi job. Controlli suggeri A.8.13 Information b A.5.30 ICT readiness business continuity.
Database clienti	Modifica non autorizzata dei dati	Permessi eccessivi o assenza di tracciamento log	4 Alto - interruzione rilevante del servizio o danno reputazionale	3 Media - evento possibile in condizioni normali	12	Alto	Responsabile IT			Mitigare il rischio applicando il principi minimo privilegio, att MFA, riesaminando periodicamente gli a e formalizzando provisioning/deprovis Controlli suggeriti: A. Access control; A.8.5 Secure authenticatio A.8.2 Privileged acce rights.
Database clienti	Violazione della confidenzialità delle informazioni	Classificazione dati assente o canali di invio non protetti	4 Alto - interruzione rilevante del servizio o danno reputazionale	3 Media - evento possibile in condizioni normali	12	Alto	Direzione / IT			Mitigare il rischio cor misure organizzative tecniche proporziona formalizzando contro responsabilità e riesa periodici.
Database clienti	Errore umano nella gestione documenti o dati	Procedure non formalizzate o formazione insufficiente	3 Medio - impatto operativo o economico moderato	4 Alta - evento probabile nel breve periodo	12	Alto	Responsabile di processo			Mitigare il rischio formalizzando istruzi operative, verifiche a campione e formazio periodica al persona Controlli suggeriti: A. Information security awareness, educatio training; A.5.10 Acce use of information ar other associated ass
Database clienti	Accesso non autorizzato ai dati	Password deboli o mancata MFA	4 Alto - interruzione rilevante del servizio o	3 Media - evento possibile in	12	Alto	Responsabile IT			Mitigare il rischio applicando il principi minimo privilegio, att MFA, riesaminando

Asset	Minaccia	Vulnerabilità	Impatto	Probabilità	Score	Livello	Responsabile	Funzione	Persona	Trattamento
			danno reputazionale	condizioni normali						periodicamente gli a e formalizzando provisioning/deprovis Controlli suggeriti: A. Access control; A.8.5 Secure authenticatio A.8.2 Privileged acce rights.
-	Smarrimento o furto di dispositivo	Cifratura assente e mancata gestione dispositivi mobili	4 Alto - interruzione rilevante del servizio o danno reputazionale	2 Bassa - evento poco probabile	8	Medio	Responsabile IT			Mitigare il rischio cor misure organizzative tecniche proporziona formalizzando contro responsabilità e riesa periodici.
-	Interruzione servizio da fornitore SaaS / cloud	Mancanza di SLA o di soluzioni alternative	4 Alto - interruzione rilevante del servizio o danno reputazionale	2 Bassa - evento poco probabile	8	Medio	Responsabile IT			Trasferire o mitigare rischio definendo SL misure contrattuali, r di continuità del forni soluzioni alternative. Controlli suggeriti: A. Information security supplier relationship A.5.23 Information s for use of cloud serv