SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Procedure SGSI

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-PRC-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

Pack procedure SGSI

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.

PACK PROCEDURE SGSI

Le procedure riportate di seguito definiscono i controlli operativi minimi per la gestione del SGSI.

PROC-BCK-001 - Backup e ripristino

Procedura Backup e ripristino

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-CLS-001 - Classificazione delle informazioni

Procedura Classificazione delle informazioni

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-BCP-001 - Continuità operativa e continuità ICT

Procedura Continuità operativa e continuità ICT

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-ACC-001 - Gestione accessi

Procedura Gestione accessi

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-AST-001 - Gestione asset informativi

Procedura Gestione asset informativi

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-SUP-001 - Gestione fornitori e terze parti

Procedura Gestione fornitori e terze parti

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-INC-001 - Gestione incidenti di sicurezza

Procedura Gestione incidenti di sicurezza

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.

PROC-VUL-001 - Gestione vulnerabilità

Procedura Gestione vulnerabilità

Scopo
Stabilire regole operative coerenti con il SGSI di GMK SISTEMI SRL.

Campo di applicazione
Tutte le attività incluse nel campo di applicazione del SGSI.

Riferimenti al contesto
Contesto interno da dettagliare.

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 (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (in_progress)
- 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.
- Evitare: 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.
- Accettare: 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.