DOSSIER EVIDENZE

Riesame risultanze Stage 1 e preparazione Stage 2

ISO 9001:2015 - ISO/IEC 27001:2022

SICULA SYSTEM SRL

Pacchetto di evidenze documentali per la chiusura dei rilievi emersi nello Stage 1 e la preparazione allo Stage 2

Organizzazione	SICULA SYSTEM SRL
Sede legale e operativa	Via della Costituzione sn, 97015 Modica (RG)
Unita locale / ufficio	Via Cozzo Rotondo 64A, 97015 Modica (RG)
Campo di applicazione	Erogazione di servizi di accesso a Internet
Norme	ISO 9001:2015 - ISO/IEC 27001:2022
Rif. cliente	ST120260427001
Referente	Giorgio Garrafa - CEO / Top Management
Data predisposizione	27/04/2026
Stato documento	Bozza operativa da validare e approvare

Avvertenza di utilizzo: il presente PDF contiene evidenze documentali, modelli compilabili e registrazioni di predisposizione. Le registrazioni relative ad attivita effettivamente svolte - ad esempio audit interno, formazione, test backup, riesame direzione, gestione reclami o incidenti - devono essere completate con dati reali, date effettive, firme/approvazioni e allegati oggettivi prima della presentazione allo Stage 2.

Indice delle evidenze incluse

Codice	Evidenza	Finalita
E00	Matrice di correlazione rilievi Stage 1 - evidenze	Mostrare il collegamento tra rilievi, azioni e documenti prodotti
E01	Piano di azione Stage 1 - Stage 2	Gestire responsabilita, scadenze, output attesi e stato di chiusura
E02	Analisi contesto, parti interessate, rischi e opportunita	Coprire ISO 9001/27001 clausole 4.1, 4.2 e 6.1
E03	Mappa processi SGQ/SGSI e interazioni	Coprire identificazione, sequenza e interazione dei processi
E04	Campo di applicazione e confini	Confermare sedi, processi, servizi e confini del sistema
E05	Politica integrata Qualita e Sicurezza Informazioni	Rendere disponibile una politica coerente con scope e contesto
E06	Obiettivi, KPI e piano di monitoraggio	Dimostrare obiettivi misurabili, monitorati e comunicati
E07	Programma audit interno e checklist	Pianificare audit interno integrato prima dello Stage 2
E08	Verbale di riesame della direzione - schema compilabile	Formalizzare input, output, decisioni e azioni del riesame
E09	Competenze, formazione e consapevolezza	Dimostrare competenze, piano formazione e awareness
E10	Valutazione fornitori e controllo servizi esterni	Dimostrare qualifica, monitoraggio e requisiti contrattuali fornitori
E11	Feedback cliente e gestione reclami	Dimostrare monitoraggio soddisfazione e gestione sistematica reclami
E12	SGSI: criteri rischio, risk assessment e trattamento	Coprire clausole ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3
E13	SoA sintetica e accettazione rischi residui	Predisporre dichiarazione di applicabilita e decisione sui rischi residui
E14	Procedure Annex A: incidenti, continuita, accessi, backup, sviluppo sicuro	Colmare le evidenze Annex A richieste prima dello Stage 2
E15	Registro evidenze da allegare allo Stage 2	Checklist finale per completamento del fascicolo

Premessa - risultanze Stage 1 utilizzate

Il dossier e stato predisposto a partire dalle risultanze riportate nel Rapporto di Audit Stage 1 di SICULA SYSTEM SRL. Il rapporto identifica, per ISO 9001, carenze/gap e osservazioni su manuale integrato, analisi del contesto, politica qualita, audit interno, riesame della direzione, obiettivi qualita, formazione, valutazione fornitori e feedback/reclami. Per ISO/IEC 27001 risultano inoltre da consolidare elementi relativi a contesto, parti interessate, risk assessment, piano di trattamento, SoA, accettazione rischi residui, pianificazione modifiche, comunicazione, controllo informazioni documentate, monitoraggio, azioni correttive e alcuni controlli Annex A.

L'esito Stage 1 riporta la raccomandazione al passaggio allo Stage 2, ma segnala aree di preoccupazione da verificare o chiudere prima dello Stage 2. Il presente pacchetto consente di organizzare in modo coerente le evidenze richieste.

Nota importante: il documento non sostituisce le evidenze operative reali. Ogni sezione deve essere riesaminata dal cliente, completata con dati effettivi, firmata/approvata ove necessario e mantenuta sotto controllo documentale.

E00 - Matrice di correlazione rilievi Stage 1 - evidenze predisposte

Rilievo / area Stage 1	Norma / clausola	Evidenza da presentare allo Stage 2	Codice
Manuale Qualita ISO 9001 / Manuale Integrato non pienamente disponibile o non aggiornato	ISO 9001 clausole 4-10	Manuale o descrizione integrata del sistema, mappa processi, procedure richiamate, controllo revisioni e approvazione	E03, E04, E05, E06, E07, E08
Analisi del contesto e rischi/opportunita non pienamente disponibile o da aggiornare	ISO 9001 4.1, 4.2, 6.1; ISO/IEC 27001 4.1, 4.2, 6.1	Analisi contesto interno/esterno, parti interessate, requisiti, rischi e opportunita	E02
Processi SGQ non identificati con sequenza e interazioni	ISO 9001 4.4	Mappa processi, input/output, indicatori, responsabili e interazioni	E03
Politica Qualita non pienamente disponibile o da aggiornare	ISO 9001 5.2	Politica integrata Qualita e Sicurezza Informazioni approvata dalla Direzione	E05
Obiettivi qualita non disponibili o non misurati/monitorati/comunicati	ISO 9001 6.2	Piano obiettivi con KPI, target, frequenza, responsabile e stato	E06
Piano/rapporto audit interno parziale o da aggiornare	ISO 9001 9.2; ISO/IEC 27001 9.2	Programma audit interno integrato, piano audit, checklist e rapporto da compilare a audit svolto	E07
Verbale riesame direzione assente/non disponibile	ISO 9001 9.3; ISO/IEC 27001 9.3	Verbale riesame direzione con input, decisioni, azioni, risorse e firma Top Management	E08
Registrazioni formazione e competenza parziali	ISO 9001 7.2, 7.3; ISO/IEC 27001 7.2, 7.3	Matrice competenze, piano formazione, registro presenze/awareness	E09
Valutazione fornitori / controllo esterni parziale	ISO 9001 8.4; Annex A 5.19-5.22	Registro fornitori critici, criteri qualifica e rivalutazione, requisiti sicurezza contrattuali	E10
Feedback clienti / reclami parziali	ISO 9001 9.1.2; 10.2	Registro feedback/reclami, tempi presa in carico, azioni e chiusura	E11
SoA e decisione rischi residui non disponibili	ISO/IEC 27001 6.1.3	SoA sintetica, piano trattamento e accettazione dei rischi residui	E12, E13
Procedure incidenti, continuita ICT, accessi, sviluppo sicuro non adeguatamente disponibili	Annex A 5.24-5.27, 5.30, 5.15-5.18, 8.2, 8.5, 8.25-8.29	Procedure operative e registri di supporto	E14

E01 - Piano di azione Stage 1 - Stage 2

Scopo: definire le azioni necessarie per chiudere le aree di preoccupazione e i gap emersi nello Stage 1, assegnando responsabilita, scadenze, evidenze oggettive e stato di completamento.

ID	Azione	Responsabile	Scadenza suggerita	Evidenza oggettiva attesa	Stato
A1	Approvare e mettere sotto controllo il Manuale/Documento descrittivo del sistema integrato SGQ-SGSI, con rinvio alle procedure applicabili.	Top Management / Resp. Sistema	Prima Stage 2	Documento approvato, indice revisioni, elenco distribuzione	Da completare
A2	Completare analisi del contesto, parti interessate, rischi e opportunita per ISP e sicurezza informazioni.	Resp. Sistema / CEO	Prima Stage 2	Analisi contesto, matrice parti interessate, registro rischi/opportunita	Da completare
A3	Formalizzare mappa processi, sequenza, interazioni, input/output, KPI e responsabilita.	Resp. Sistema	Prima Stage 2	Mappa processi e schede processo approvate	Da completare
A4	Approvare Politica integrata Qualita e Sicurezza Informazioni e comunicarla al personale.	CEO	Prima Stage 2	Politica firmata, comunicazione interna, pubblicazione/affissione	Da completare
A5	Definire obiettivi qualita e sicurezza informazioni con indicatori misurabili e piano di monitoraggio.	CEO / Resp. Sistema	Prima Stage 2	Piano obiettivi, KPI, target e report monitoraggio	Da completare
A6	Eseguire audit interno integrato SGQ-SGSI e predisporre rapporto con eventuali NC/azioni correttive.	Auditor interno qualificato	Prima Stage 2	Programma, piano, checklist, rapporto audit, azioni correttive	Da pianificare
A7	Condurre riesame della direzione integrato e registrare decisioni e azioni.	CEO	Dopo audit interno e prima Stage 2	Verbale riesame approvato e piano azioni	Da pianificare
A8	Completare registro formazione/competenze e awareness security.	Resp. Sistema / HR	Prima Stage 2	Matrice competenze, piano formazione, attestazioni/presenze	Da completare
A9	Completare qualifica/rivalutazione fornitori critici e requisiti contrattuali sicurezza.	Acquisti / Resp. Sistema	Prima Stage 2	Registro fornitori, valutazioni, contratti/ordini con requisiti	Da completare
A10	Attivare registro feedback/reclami e modalita di trattamento.	Customer support	Prima Stage 2	Registro reclami/feedback, eventuali ticket e chiusure	Da completare
A11	Completare risk assessment SGSI, piano trattamento, SoA e accettazione rischi residui.	Resp. SGSI / CEO	Prima Stage 2	Risk assessment, RTP, SoA, approvazione rischi residui	Da completare
A12	Formalizzare procedure Annex A: incidenti, continuita ICT, accessi, backup, sviluppo sicuro/non applicabilita.	Resp. IT / Resp. SGSI	Prima Stage 2	Procedure, registri, test backup/continuita, elenco utenze	Da completare

Firma presa in carico Top Management: _____ Data: ____ / ____ / _____

E02 - Analisi del contesto, parti interessate, rischi e opportunita

Campo di applicazione: erogazione di servizi di accesso a Internet, incluse gestione operativa, assistenza tecnica, manutenzione, supporto al cliente e gestione delle infrastrutture e delle informazioni necessarie al servizio ISP.

Contesto interno ed esterno

Categoria	Fattore rilevante	Impatto sul sistema di gestione	Presidio / evidenza
Interno	Organizzazione di piccole dimensioni con n. 4 addetti e forte concentrazione di competenze operative.	Necessita ruoli chiari, deleghe, sostituzioni e controllo documentale essenziale ma efficace.	Organigramma, matrice ruoli/responsabilita, matrice competenze
Interno	Erogazione servizi ISP con dipendenza da infrastrutture, apparati, reti, sistemi informativi e fornitori tecnici.	La qualita del servizio dipende da continuita, disponibilita, manutenzione e gestione fornitori.	Mappa processi, registro asset, registro fornitori, piani manutenzione
Interno	Gestione di informazioni clienti, contratti, dati tecnici e dati personali.	Necessita controllo accessi, privacy, sicurezza informazioni, backup e protezione dati.	Policy security, registro accessi, DPIA/registro trattamenti ove applicabile, backup plan
Esterno	Normativa comunicazioni elettroniche, autorizzazioni/licenze, regolazione AGCOM, privacy e sicurezza reti.	Necessario monitorare requisiti cogenti e mantenere conformita documentata.	Registro requisiti cogenti e riesame periodico
Esterno	Aspettative clienti su continuita, rapidita assistenza, stabilita connessione e trasparenza contrattuale.	Necessita KPI di servizio, gestione reclami, comunicazioni e misurazione soddisfazione.	SLA, ticket, registro reclami, survey clienti
Esterno	Rischi cyber, indisponibilita servizi, guasti apparati, interruzioni energia/connettivita.	Necessita risk assessment, controlli Annex A, backup e continuita operativa ICT.	Risk assessment, BCP, procedure incidenti, test backup

Parti interessate e requisiti

Parte interessata	Bisogni / aspettative	Requisiti rilevanti	Monitoraggio
Clienti / utenti finali	Connessione disponibile, assistenza tempestiva, trasparenza, protezione dati.	Contratti, SLA, privacy, gestione reclami, continuita servizio.	Ticket, reclami, survey, KPI servizio
Top Management	Controllo dei processi, riduzione disservizi, conformita, crescita sostenibile.	Obiettivi, riesami, risorse, miglioramento continuo.	Riesame direzione, KPI, audit interni
Personale interno	Ruoli chiari, strumenti adeguati, formazione e consapevolezza.	Competenze, sicurezza, istruzioni operative.	Matrice competenze, formazione, colloqui
Fornitori tecnici	Requisiti chiari, ordini/contratti, comunicazioni operative.	Sicurezza supply chain, qualifica, monitoraggio performance.	Valutazione e rivalutazione fornitori
Autorita / enti regolatori	Conformita autorizzativa, privacy, sicurezza, comunicazioni elettroniche.	Leggi e regolamenti applicabili, conservazione evidenze.	Registro requisiti cogenti, verifiche periodiche
Organismo di certificazione	Sistema documentato, conforme, efficace e verificabile.	ISO 9001:2015, ISO/IEC 27001:2022, evidenze oggettive.	Audit, azioni correttive, riesami

Registro iniziale rischi e opportunita SGQ

ID	Rischio / opportunita	Processo	Effetto potenziale	Trattamento / azione
RQ1	Interruzione o degrado del servizio Internet	Erogazione ISP	Disservizi, reclami, perdita fiducia cliente	Monitoraggio rete, manutenzione, escalation, continuita ICT
RQ2	Documentazione non aggiornata o non controllata	SGQ/SGSI	Incoerenza operativa e NC in audit	Procedura controllo documenti, lista documenti, revisioni
RQ3	Competenze non formalizzate	Risorse umane	Dipendenza da singole persone, errori operativi	Matrice competenze, piano formazione e affiancamento
RQ4	Fornitori critici non monitorati	Acquisti/outsourcing	Impatti su continuita e sicurezza servizio	Qualifica e rivalutazione fornitori, requisiti contrattuali
O1	Standardizzazione ticket e KPI	Customer support	Miglioramento tempi risposta e tracciabilita	Adozione registro/ticketing e analisi mensile
O2	Integrazione ISO 9001 e ISO 27001	Governance	Riduzione duplicazioni e maggiore controllo	Manuale integrato, audit e riesame congiunti

Approvazione analisi contesto: CEO _____ Data: ____ / ____ / _____

E03 - Mappa processi SGQ/SGSI e interazioni

La seguente mappa documenta processi, sequenza e interazioni del sistema integrato, rispondendo ai gap Stage 1 relativi all'identificazione dei processi SGQ e al riesame delle attivita sito-specifiche.

Macroprocesso	Processi inclusi	Input principali	Output / registrazioni	KPI suggeriti
Direzione e governance	Contesto, parti interessate, politica, obiettivi, ruoli, riesame direzione, allocazione risorse.	Strategia, requisiti clienti/cogenti, risultati audit, KPI, rischi.	Politica, obiettivi, riesame, piani azione.	% obiettivi raggiunti; azioni chiuse nei tempi
Commerciale e gestione cliente	Richieste cliente, contratti, definizione requisiti servizio, comunicazioni, reclami.	Richieste/contratti clienti, requisiti legali e tecnici.	Contratti, ticket, reclami, comunicazioni.	Tempo risposta; reclami chiusi; soddisfazione cliente
Erogazione servizi ISP	Attivazione, gestione operativa rete, monitoraggio servizio, interventi tecnici, supporto, manutenzione.	Contratti, configurazioni, apparati, risorse tecniche.	Servizio erogato, ticket intervento, report uptime, manutenzioni.	Uptime; tempo risoluzione; guasti ricorrenti
Gestione infrastrutture e asset	Inventario asset, manutenzione apparati, backup, accessi, sicurezza endpoint/rete.	Asset, configurazioni, requisiti sicurezza.	Inventario, registri manutenzione, log accessi, test backup.	% asset inventariati; test backup OK
Gestione SGSI	Risk assessment, trattamento rischi, SoA, incident management, continuita operativa, awareness.	Asset, minacce, vulnerabilita, requisiti Annex A.	Risk assessment, RTP, SoA, incident register, BCP.	Rischi trattati; incidenti; test continuita
Acquisti e fornitori	Qualifica, ordini, contratti, monitoraggio fornitori critici, requisiti security.	Esigenze operative, requisiti tecnici/security.	Elenco fornitori, valutazioni, accordi.	% fornitori qualificati; valutazione media
Risorse umane e competenze	Matrice competenze, formazione, consapevolezza, affiancamento.	Ruoli, requisiti competenza, gap rilevati.	Piano formazione, registri presenze, valutazioni efficacia.	Ore formazione; % formazione completata
Valutazione prestazioni e miglioramento	Audit interni, monitoraggio KPI, NC/AC, analisi dati, miglioramento.	KPI, reclami, audit, incidenti, feedback.	Rapporti audit, NC, azioni correttive, riesame.	% azioni chiuse; NC ripetute

Sequenza sintetica dei processi

Contesto e requisiti -> Politica e obiettivi -> Pianificazione rischi/opportunita -> Gestione richieste cliente e requisiti servizio -> Erogazione servizi ISP -> Monitoraggio prestazioni e sicurezza -> Gestione reclami/incidenti/NC -> Audit interno -> Riesame direzione -> Miglioramento.

Scheda processo tipo - Erogazione servizi ISP

Voce	Contenuto
Responsabile	Responsabile tecnico / CEO, con supporto del personale operativo
Input	Contratto cliente, richiesta attivazione/intervento, requisiti tecnici, dati cliente, disponibilita infrastruttura
Attivita	Presa in carico, configurazione/attivazione, monitoraggio, supporto tecnico, manutenzione, registrazione ticket/intervento
Output	Servizio Internet erogato, evidenza attivazione, ticket chiuso, report tecnico, eventuale comunicazione cliente
Rischi	Disservizio, errore configurazione, accesso non autorizzato, indisponibilita apparati/fornitori, perdita dati
Controlli	Access control, backup, monitoraggio rete, escalation, manutenzione, fornitori qualificati, logging
KPI	Uptime mensile, tempo medio presa in carico, tempo medio risoluzione, numero reclami tecnici, incidenti security

E04 - Campo di applicazione, confini e attivita sito-specifiche

Scope IT: Erogazione di servizi di accesso a Internet.

Scope EN: Provision of Internet access services.

Il sistema integrato si applica ai processi aziendali relativi all'erogazione di servizi di accesso a Internet, comprese le attivita di gestione operativa, assistenza tecnica, manutenzione, supporto al cliente e gestione delle infrastrutture e delle informazioni necessarie all'erogazione del servizio.

Sito	Indirizzo	Attivita incluse	Note di confine
Sede principale / legale e operativa	Via della Costituzione sn, 97015 Modica (RG)	Direzione, gestione processi, amministrazione, gestione servizi ISP, gestione clienti e supporto.	Inclusa nel campo di applicazione SGQ/SGSI
Unita locale / ufficio	Via Cozzo Rotondo 64A, 97015 Modica (RG)	Attivita operative e/o di supporto connesse ai servizi ISP.	Inclusa nel campo di applicazione; verificare eventuali asset e attivita sito-specifiche

Applicabilita ISO 9001 - progettazione e sviluppo

Allo stato delle informazioni disponibili, il requisito ISO 9001:2015 punto 8.3 potra essere dichiarato non applicabile solo se l'organizzazione dimostra di non progettare o sviluppare nuovi servizi, limitandosi all'erogazione e gestione di servizi ISP secondo requisiti tecnici, contrattuali e regolamentari gia definiti. La giustificazione deve essere documentata e riesaminata allo Stage 2.

Applicabilita ISO/IEC 27001 - Annex A

Per ISO/IEC 27001 non si prevedono esclusioni dal sistema di gestione. L'applicabilita o non applicabilita dei controlli Annex A deve essere motivata nella Dichiarazione di Applicabilita in coerenza con risk assessment, piano di trattamento e requisiti cogenti/contrattuali.

E05 - Politica integrata Qualita e Sicurezza delle Informazioni

La Direzione di SICULA SYSTEM SRL, coerentemente con il campo di applicazione relativo all'erogazione di servizi di accesso a Internet, si impegna a mantenere un sistema di gestione integrato per la qualita e la sicurezza delle informazioni idoneo a garantire servizi affidabili, conformi ai requisiti applicabili e orientati alla soddisfazione del cliente.

Principi della politica

- Assicurare la conformita ai requisiti legali, regolamentari, autorizzativi, contrattuali e normativi applicabili ai servizi ISP.
- Erogare servizi di accesso a Internet con attenzione a continuita, disponibilita, tempestivita di supporto e gestione dei disservizi.
- Proteggere riservatezza, integrita e disponibilita delle informazioni gestite nell'ambito dei servizi erogati.
- Adottare un approccio basato sul rischio per la qualita del servizio, la sicurezza delle informazioni e la continuita operativa.
- Assicurare competenze, consapevolezza e responsabilita adeguate al personale e ai collaboratori coinvolti nei processi.
- Selezionare e monitorare fornitori critici in coerenza con requisiti di qualita, sicurezza, continuita e conformita.
- Monitorare obiettivi e indicatori, gestire non conformita, reclami e incidenti e promuovere il miglioramento continuo.

Obblighi della Direzione

La Direzione si impegna a rendere disponibile la presente politica alle parti interessate rilevanti, riesaminarla periodicamente, assicurare risorse adeguate, comunicare obiettivi e responsabilita e sostenere la cultura della qualita e della sicurezza delle informazioni.

Controllo documento	Dati
Codice documento	POL-INT-01
Versione	Rev. 00
Data emissione	____ / ____ / _____
Approvato da	Giorgio Garrafa - CEO / Top Management
Modalita comunicazione	Condivisione interna, affissione o pubblicazione su repository documentale controllato
Riesame previsto	Annuale o in caso di modifiche significative a servizi, rischi, norme o organizzazione

Firma approvazione: _____ Data: ____ / ____ / _____

E06 - Obiettivi, KPI e piano di monitoraggio

Gli obiettivi sono definiti in modo misurabile, coerente con la politica integrata e con i rischi/opportunita identificati. I valori iniziali e i target devono essere confermati con dati reali disponibili prima dello Stage 2.

ID	Obiettivo	Indicatore	Target suggerito	Frequenza	Responsabile	Evidenza
OQ1	Migliorare tracciabilita e gestione dei ticket/reclami cliente	% ticket/reclami registrati e chiusi con esito	>= 95% registrati; 100% reclami con azione/risposta	Mensile	Customer support	Registro ticket/reclami
OQ2	Garantire continuita e disponibilita del servizio ISP	Uptime servizio / disservizi critici	Uptime >= target contrattuale; analisi disservizi critici	Mensile	Resp. tecnico	Report monitoraggio rete
OQ3	Ridurre ritardi nella gestione interventi tecnici	Tempo medio presa in carico e risoluzione	Presa in carico entro soglia definita; trend migliorativo	Mensile	Resp. tecnico	Report ticket/interventi
OQ4	Completare controllo documentale SGQ-SGSI	% documenti chiave approvati e revisionati	100% documenti critici approvati prima Stage 2	Prima Stage 2 / trimestrale	Resp. Sistema	Lista documenti controllati
OQ5	Completare formazione e awareness sicurezza informazioni	% personale formato	100% personale interno formato	Annuale	CEO / Resp. Sistema	Registro formazione
OS1	Migliorare protezione accessi sistemi critici	% utenze censite e autorizzate	100% utenze censite; MFA ove applicabile	Trimestrale	Resp. IT	Registro accessi
OS2	Assicurare efficacia backup	% backup completati e test ripristino	Backup monitorati; almeno 1 test ripristino documentato	Mensile / semestrale	Resp. IT	Log backup e test restore
OS3	Gestire incidenti security in modo sistematico	% incidenti registrati e chiusi	100% incidenti/segnalazioni registrati e classificati	A evento / trimestrale	Resp. SGSI	Registro incidenti

Comunicazione obiettivi

Gli obiettivi devono essere comunicati al personale interessato mediante riunione interna, e-mail o repository documentale. Il monitoraggio deve essere riesaminato durante audit interno e riesame della direzione.

Approvazione piano obiettivi: CEO _____ Data: ____ / ____ / _____

E07 - Programma audit interno integrato e checklist

Il programma audit interno deve essere completato prima dello Stage 2 per verificare conformita ed efficacia di SGQ e SGSI. Le evidenze finali dovranno includere: programma, piano audit, checklist compilata, rapporto audit, eventuali NC/azioni correttive e verifica efficacia.

Elemento	Contenuto previsto
Periodo audit	Da pianificare prima dello Stage 2
Norme	ISO 9001:2015; ISO/IEC 27001:2022; procedure interne; requisiti cogenti e contrattuali
Siti inclusi	Via della Costituzione sn, Modica (RG); Via Cozzo Rotondo 64A, Modica (RG), ove applicabile
Processi inclusi	Direzione, commerciale/cliente, erogazione servizi ISP, supporto tecnico, infrastrutture/asset, fornitori, formazione, SGSI, miglioramento
Auditor interno	Da nominare, competente e indipendente rispetto alle attivita verificate ove possibile
Output	Rapporto audit interno integrato con conclusioni, rilievi, azioni correttive e responsabilita

Checklist sintetica per audit interno

Area	Domande minime di verifica	Evidenze da campionare	Esito
Contesto e scope	Sono aggiornati contesto, parti interessate, campo di applicazione e confini?	Analisi contesto, parti interessate, scope, siti	C / NC / O
Processi SGQ/SGSI	Sono definiti processi, sequenza, interazioni, responsabilita e KPI?	Mappa processi, schede processo, KPI	C / NC / O
Leadership e politica	Politica approvata, comunicata e coerente con il servizio ISP?	Politica firmata, comunicazione interna	C / NC / O
Obiettivi	Obiettivi misurabili, monitorati, comunicati e coerenti con rischi?	Piano obiettivi, report KPI	C / NC / O
Operativita ISP	Sono gestiti attivazioni, supporto, manutenzione e disservizi?	Ticket, rapporti intervento, report uptime	C / NC / O
Fornitori	Fornitori critici qualificati e monitorati?	Registro fornitori, valutazioni, contratti	C / NC / O
Competenze	Competenze e formazione sono definite e registrate?	Matrice competenze, presenze, attestati	C / NC / O
SGSI rischio	Risk assessment, RTP, SoA e rischi residui sono approvati?	Risk assessment, SoA, piano trattamento	C / NC / O
Annex A	Sono disponibili e attuati controlli su asset, accessi, backup, incidenti, continuita?	Registri asset/accessi/backup/incidenti, BCP	C / NC / O
Miglioramento	NC, reclami, incidenti e azioni correttive sono gestiti?	Registro NC/AC, reclami, incidenti	C / NC / O

Firma auditor interno: _____ Data audit: ____ / ____ / _____

E08 - Verbale di riesame della direzione - schema compilabile

Questo schema consente di predisporre il verbale richiesto prima dello Stage 2. Deve essere compilato dopo avere completato almeno audit interno, monitoraggio obiettivi, risk assessment SGSI e raccolta dati disponibili.

Sezione	Contenuto da riesaminare	Output / decisione da registrare
Partecipanti	CEO / Top Management; Resp. Sistema; Resp. tecnico/IT; eventuali funzioni coinvolte.	Elenco partecipanti e firme
Stato azioni precedenti	Azioni da Stage 1 e azioni interne aperte.	Conferma chiusura o aggiornamento scadenze
Cambiamenti interni/esterni	Normativa, servizi, siti, fornitori, rischi, tecnologie, clienti.	Necessita modifiche al SGQ/SGSI
Prestazioni qualita	KPI servizi ISP, ticket, reclami, non conformita, soddisfazione cliente.	Azioni di miglioramento e target aggiornati
Prestazioni sicurezza informazioni	Incidenti, eventi, backup, accessi, risk treatment, continuita ICT.	Decisioni su controlli, risorse, rischi residui
Audit interno	Risultati audit, NC, osservazioni e opportunita.	Approvazione piano azioni correttive
Fornitori	Performance fornitori critici, criticita, contratti.	Conferma/rimozione fornitori, nuove clausole security
Risorse e competenze	Formazione, consapevolezza, fabbisogni risorse.	Piano formazione e risorse necessarie
Obiettivi	Stato raggiungimento obiettivi qualita e security.	Conferma o revisione target
Miglioramento	Azioni preventive/correttive e opportunita.	Piano miglioramento approvato

Delibere minime suggerite

- Approvazione del campo di applicazione SGQ/SGSI: erogazione di servizi di accesso a Internet.
- Approvazione della Politica integrata Qualita e Sicurezza Informazioni.
- Approvazione degli obiettivi e dei KPI per il periodo successivo.
- Approvazione del risk assessment SGSI, del piano di trattamento e della SoA.
- Accettazione formale dei rischi residui nei limiti dei criteri stabiliti.
- Assegnazione delle risorse e delle responsabilita per chiudere le azioni prima dello Stage 2.

Firma CEO / Top Management: _____ Data riesame: ____ / ____ / _____

E09 - Competenze, formazione e consapevolezza

Scopo: dimostrare che l'organizzazione ha identificato le competenze necessarie per i ruoli rilevanti, ha pianificato la formazione e conserva evidenze di consapevolezza su qualita e sicurezza informazioni.

Ruolo / funzione	Competenze richieste	Evidenze accettabili	Gap / azione
CEO / Top Management	Leadership SGQ/SGSI, requisiti cliente/cogenti, riesame direzione, risk based thinking.	CV, esperienza, verbali direzione, formazione ISO	Aggiornamento ISO 9001/27001 e responsabilita direzione
Responsabile sistema integrato	Gestione documenti, audit, NC/AC, risk assessment, obiettivi, requisiti ISO.	Nomina, formazione, attestati, esperienza	Formalizzare nomina e responsabilita
Responsabile tecnico / IT	Gestione rete/asset, accessi, backup, incidenti, continuita, manutenzione.	CV, qualifiche tecniche, registri attivita	Awareness Annex A e incident response
Addetti supporto cliente/tecnico	Gestione richieste, ticket, reclami, privacy, sicurezza informazioni, istruzioni operative.	Registri formazione, affiancamento, checklist	Formazione su reclami, security e gestione dati clienti

Piano formazione minimo prima dello Stage 2

Modulo	Destinatari	Durata suggerita	Contenuti	Evidenza
Awareness ISO 9001 e processi	Tutto il personale coinvolto	1 ora	Politica qualita, processi, KPI, reclami, NC	Registro presenze / test apprendimento
Awareness ISO/IEC 27001	Tutto il personale	1 ora	Riservatezza, integrita, disponibilita, phishing, password, incidenti	Registro presenze / test
Gestione ticket, reclami e non conformita	Supporto e tecnico	1 ora	Registrazione, classificazione, tempi, azioni, chiusura	Registro formazione, esempi ticket
Incident response e backup	Resp. IT / tecnico	1-2 ore	Incidenti, escalation, log, backup, test restore	Verbale formazione, test backup

Registro presenze formazione

Data	Modulo	Partecipante	Ruolo	Firma	Esito verifica
____/____/____	_____	_____	_____	_____	OK / da ripetere
____/____/____	_____	_____	_____	_____	OK / da ripetere
____/____/____	_____	_____	_____	_____	OK / da ripetere

E10 - Valutazione fornitori e controllo servizi esterni

Scopo: garantire che i fornitori critici per la qualita del servizio ISP e per la sicurezza delle informazioni siano identificati, qualificati, monitorati e gestiti con requisiti contrattuali adeguati.

Categoria fornitore	Criteri di qualifica	Requisiti security / qualita	Frequenza rivalutazione
Connettivita / carrier / backbone	Affidabilita servizio, SLA, supporto, storico performance, conformita contrattuale.	SLA, gestione incidenti, disponibilita, comunicazioni disservizi.	Annuale o a evento critico
Fornitori apparati rete / manutenzione	Competenza tecnica, tempi intervento, disponibilita ricambi, garanzia.	Tracciabilita interventi, accessi controllati, riservatezza.	Annuale
Software / servizi cloud / hosting	Affidabilita, sicurezza, data location, supporto, backup.	DPA/privacy ove applicabile, controllo accessi, log, backup.	Annuale
Consulenti / servizi esterni	Competenza, indipendenza ove audit, riservatezza, referenze.	NDA, accessi limitati, istruzioni operative.	A incarico / annuale

Registro fornitori critici - da compilare

Fornitore	Servizio fornito	Criticita	Valutazione iniziale	Requisiti contrattuali	Esito
_____	_____	Alta / Media / Bassa	Documenti / SLA / referenze	SLA / NDA / DPA / security	Qualificato / non qualificato
_____	_____	Alta / Media / Bassa	Documenti / SLA / referenze	SLA / NDA / DPA / security	Qualificato / non qualificato
_____	_____	Alta / Media / Bassa	Documenti / SLA / referenze	SLA / NDA / DPA / security	Qualificato / non qualificato

Clausole minime suggerite per fornitori critici

- Obbligo di riservatezza e protezione delle informazioni ricevute o trattate per conto dell'organizzazione.
- Obbligo di comunicazione tempestiva di incidenti, disservizi o violazioni che possano impattare il servizio ISP.
- Livelli di servizio, tempi di intervento o canali di escalation, ove applicabili.
- Limitazione e controllo degli accessi ai sistemi/asset aziendali, ove necessari.
- Conformita a privacy, sicurezza informazioni e requisiti contrattuali pertinenti.

E11 - Feedback cliente, reclami e non conformita

Scopo: assicurare una gestione sistematica di feedback, reclami, disservizi e non conformita, con tracciabilita dalla segnalazione alla chiusura e verifica dell'efficacia delle azioni.

Fase	Descrizione	Registrazione richiesta
Ricezione	Segnalazione da cliente, e-mail, telefono, ticket, monitoraggio o altro canale.	ID ticket/reclamo, data, cliente, descrizione
Classificazione	Distinguere richiesta, reclamo, disservizio, non conformita, incidente security.	Categoria, priorita, impatto
Presa in carico	Assegnare responsabile e tempi previsti.	Responsabile, data presa in carico, SLA interno
Trattamento	Eseguire analisi causa, correzione e, se necessario, azione correttiva.	Azioni, evidenze tecniche, comunicazioni
Chiusura	Confermare risoluzione e comunicare esito al cliente.	Data chiusura, esito, soddisfazione
Analisi periodica	Riesaminare trend e ricorrenze durante riesame direzione.	Report KPI, trend reclami, azioni preventive

Registro reclami/feedback - da compilare

ID	Data	Cliente	Tipo	Descrizione	Responsabile	Azione	Chiusura
R-____	____/____/____	_____	Feedback/Reclamo/NC	_____	_____	_____	Aperto/Chiuso
R-____	____/____/____	_____	Feedback/Reclamo/NC	_____	_____	_____	Aperto/Chiuso

In assenza di reclami nel periodo, registrare comunque: "Nessun reclamo ricevuto nel periodo ____ / ____ / _____ - ____ / ____ / _____" e mantenere evidenza dei canali disponibili per il cliente.

E12 - SGSI: criteri di rischio, risk assessment e trattamento

La metodologia seguente consente di documentare criteri, valutazione e trattamento dei rischi per la sicurezza delle informazioni, in coerenza con ISO/IEC 27001:2022 clausole 6.1.2, 6.1.3, 8.2 e 8.3.

Elemento	Criterio proposto
Scala probabilita	1 remota; 2 bassa; 3 media; 4 alta; 5 molto alta
Scala impatto	1 trascurabile; 2 minore; 3 significativo; 4 grave; 5 critico
Indice rischio	R = probabilita x impatto
Soglie	1-4 basso; 5-9 medio; 10-15 alto; 16-25 critico
Criterio accettazione	Rischi bassi accettabili; medi da monitorare/trattare; alti e critici da trattare con piano approvato
Opzioni trattamento	Mitigare, trasferire, evitare, accettare con motivazione documentata
Riesame	Almeno annuale o a fronte di incidenti, modifiche significative, nuovi asset/servizi o nuovi requisiti

Registro rischi SGSI iniziale

ID	Asset / processo	Minaccia	Vulnerabilita	R	Trattamento	Controlli Annex A
RS1	Rete / servizi ISP	Indisponibilita servizio	Dipendenza da apparati/fornitori e guasti tecnici	Alto	Monitoraggio, manutenzione, escalation, continuita ICT	5.30, 8.6, 8.14
RS2	Sistemi e account	Accesso non autorizzato	Utenze non censite o password deboli	Alto	Registro accessi, policy password/MFA, review periodica	5.15-5.18, 8.2, 8.5
RS3	Dati cliente	Perdita/alterazione dati	Backup o ripristino non testati	Alto	Piano backup, test restore, protezione storage	8.13, 5.33, 5.34
RS4	Incidenti security	Rilevazione tardiva o gestione non coordinata	Assenza procedura e registro incidenti	Medio/ Alto	Procedura incident response, ruoli, registro incidenti	5.24-5.27
RS5	Fornitori critici	Disservizio o compromissione supply chain	Requisiti security non formalizzati	Medio/ Alto	Valutazione fornitori, clausole, monitoraggio	5.19-5.22
RS6	Postazioni/endpoint	Malware o errore umano	Awareness incompleta, controlli endpoint non documentati	Medio	Formazione, aggiornamenti, protezione endpoint, backup	6.3, 8.7, 8.8
RS7	Modifiche tecniche	Errore di configurazione	Change non formalizzato	Medio	Registro modifiche, approvazione e rollback	8.9, 8.32

Piano trattamento rischio - tracciato minimo

ID rischio	Azione trattamento	Responsabile	Scadenza	Evidenza attuazione	R residuo
RS1	Formalizzare BCP/continuita ICT e procedure escalation disservizi	Resp. IT	Prima Stage 2	BCP approvato, test/verbale	Da valutare
RS2	Censire utenze e formalizzare policy accessi/password/MFA	Resp. IT	Prima Stage 2	Registro accessi, policy, review account	Da valutare
RS3	Documentare piano backup e almeno un test restore	Resp. IT	Prima Stage 2	Log backup, verbale test ripristino	Da valutare
RS4	Approvare procedura gestione incidenti e registro incidenti	Resp. SGSI	Prima Stage 2	Procedura, registro, comunicazione interna	Da valutare
RS5	Rivalutare fornitori critici e includere requisiti security	Acquisti/CEO	Prima Stage 2	Registro fornitori e clausole	Da valutare

E13 - SoA sintetica e accettazione rischi residui

La Dichiarazione di Applicabilita deve elencare i controlli Annex A applicabili/non applicabili, la motivazione, lo stato di attuazione e le evidenze. La tabella seguente e una SoA sintetica mirata ai controlli emersi nello Stage 1; dovra essere completata con tutti i controlli Annex A applicabili.

Controllo Annex A	Applicabilita	Motivazione	Stato / evidenza richiesta
5.9 Inventario asset informativi	Applicabile	Necessario per gestire informazioni, sistemi e apparati del servizio ISP.	Registro asset disponibile/da aggiornare con owner e criticita
5.15-5.18 Controllo accessi e diritti	Applicabile	Accessi a sistemi, rete e dati cliente devono essere autorizzati e riesaminati.	Policy accessi, registro utenze, review periodica
5.19-5.22 Sicurezza fornitori	Applicabile	Fornitori tecnici e servizi esterni possono incidere su qualita e sicurezza.	Registro fornitori, requisiti contrattuali security
5.24-5.27 Gestione incidenti	Applicabile	Incidenti security e disservizi richiedono gestione strutturata e tracciata.	Procedura incidenti, registro incidenti, ruoli escalation
5.30 Prontezza ICT per continuita operativa	Applicabile	Il servizio ISP richiede continuita e ripristino in caso di evento critico.	BCP/ICT continuity, test e riesame
8.2 Diritti di accesso privilegiato	Applicabile	Account amministrativi su rete/sistemi necessitano controllo rafforzato.	Elenco admin, autorizzazioni, review
8.5 Autenticazione sicura	Applicabile	Riduce rischio accessi non autorizzati.	Policy password/MFA, configurazioni
8.13 Backup	Applicabile	Necessario per disponibilita e ripristino dati/sistemi.	Piano backup, log, test restore
8.25-8.29 Sviluppo sicuro	Da valutare	Applicabile se l'organizzazione sviluppa software o personalizzazioni significative; non applicabile se non vi e sviluppo.	Motivazione documentata oppure procedura sviluppo sicuro/test

Accettazione rischi residui

La Direzione accetta i rischi residui solo se coerenti con i criteri di accettazione definiti, documentati nel risk assessment e riesaminati periodicamente. L'accettazione non e ammessa per rischi residui alti/critici senza piano di trattamento approvato, risorse assegnate e scadenza definita.

ID rischio	Rischio residuo	Motivazione accettazione / ulteriore trattamento	Decisione Direzione	Firma
RS__	Basso / Medio / Alto	_____	Accettato / non accettato	_____
RS__	Basso / Medio / Alto	_____	Accettato / non accettato	_____

E14 - Procedure Annex A: incidenti, continuita, accessi, backup, sviluppo sicuro

Le procedure seguenti sono predisposte come evidenza documentale minima da approvare e attuare prima dello Stage 2. Ogni procedura deve essere integrata con registrazioni reali di attuazione.

E14.1 Procedura gestione incidenti e registro incidenti

Fase	Descrizione operativa	Evidenza
Rilevazione	Ogni evento anomalo su reti, sistemi, dati, account, fornitori o clienti deve essere segnalato al responsabile SGSI/IT.	Segnalazione, ticket o e-mail
Classificazione	Classificare come evento, incidente, near miss, violazione dati personali, disservizio operativo.	Registro incidenti con categoria e impatto
Contenimento	Isolare sistemi, revocare accessi, bloccare account, applicare workaround, informare fornitori se necessario.	Log azioni e tempi
Analisi e ripristino	Identificare causa, ripristinare servizio, verificare integrita e disponibilita.	Rapporto tecnico
Comunicazioni	Valutare obblighi verso clienti, autorita, Garante privacy o altri soggetti in base a impatto e natura evento.	Registro comunicazioni
Chiusura e lessons learned	Registrare azioni correttive e aggiornare risk assessment/controlli.	Chiusura incidente e AC

E14.2 Piano di continuita operativa e prontezza ICT

Scenario	Impatto	Strategia di continuita/ripristino	Evidenza test
Guasto apparato/rete critica	Interruzione servizio ISP o degrado con reclami	Escalation tecnica, apparato sostitutivo, fornitore, comunicazione cliente se necessario	Verbale test / simulazione
Indisponibilita sistemi di supporto/ticket	Perdita tracciabilita richieste e interventi	Canale alternativo, backup dati, registro temporaneo manuale	Test accesso backup
Perdita dati/configurazioni	Impossibilita ripristino rapido	Backup configurazioni e dati critici; test ripristino periodico	Log backup + test restore
Indisponibilita personale chiave	Ritardi in assistenza o gestione incidenti	Sostituti, istruzioni operative, contatti escalation	Matrice sostituzioni

E14.3 Politica controllo accessi e autenticazione

- Ogni account deve essere nominativo, autorizzato da responsabile competente e censito in registro utenze.
- Gli account privilegiati devono essere limitati al personale autorizzato, riesaminati periodicamente e protetti con misure rafforzate.
- Le credenziali devono essere personali, non condivise e gestite con regole minime di complessita, cambio o MFA ove applicabile.
- Le cessazioni o cambi ruolo devono comportare revisione o revoca tempestiva degli accessi.
- Gli accessi di fornitori esterni devono essere temporanei, autorizzati e tracciati ove tecnicamente possibile.

Utente	Sistema/asset	Profilo	Autorizzato da	Data attivazione	Data review	Esito
_____	_____	Admin/User	_____	____/____/_____	____/____/_____	Confermato/Revocato
_____	_____	Admin/User	_____	____/____/_____	____/____/_____	Confermato/Revocato

E14.4 Piano backup e test di ripristino

Elemento	Regola minima
Oggetto backup	Dati clienti/contratti, configurazioni apparati, documentazione SGQ/SGSI, sistemi/ticket ove applicabile
Frequenza	Da definire in base a criticita; minimo giornaliera/settimanale per dati critici ove applicabile
Protezione	Accesso limitato, segregazione, cifratura ove applicabile, protezione da cancellazioni non autorizzate
Monitoraggio	Controllo esito backup e registrazione anomalie
Test ripristino	Almeno semestrale/annuale o dopo modifiche rilevanti; registrare data, oggetto, esito, tempi e criticita

E14.5 Sviluppo sicuro - valutazione applicabilita

Se SICULA SYSTEM SRL non svolge sviluppo software, personalizzazioni applicative o test di sicurezza su software sviluppato internamente, i controlli Annex A 8.25-8.29 possono essere motivati come non applicabili nella SoA. Se invece vengono sviluppati o modificati software, script, portali, sistemi o automazioni rilevanti, devono essere definite regole per requisiti security, controllo versioni, test, segregazione ambienti e gestione vulnerabilita.

E15 - Registro evidenze da allegare allo Stage 2

Checklist operativa per verificare che il fascicolo da presentare allo Stage 2 sia completo, controllato e coerente con le risultanze dello Stage 1.

Evidenza	Documento / registrazione	Stato	Note
Campo di applicazione	Scope IT/EN, sedi, confini, applicabilita 8.3 e Annex A	Da verificare	Coerente con servizio ISP
Manuale / documento sistema integrato	Manuale o descrizione processi + procedure richiamate	Da completare	Inserire codice, rev., approvazione
Analisi contesto e parti interessate	Matrice contesto, parti interessate, requisiti, rischi/opportunita	Da completare	E02
Mappa processi	Sequenza, interazioni, responsabilita, KPI	Da completare	E03
Politica integrata	Politica firmata e comunicata	Da approvare	E05
Obiettivi	Piano obiettivi qualita/security con KPI e target	Da approvare	E06
Audit interno	Programma, piano, checklist, rapporto, NC/AC	Da svolgere	E07
Riesame direzione	Verbale con input/output e azioni	Da svolgere	E08
Competenze/formazione	Matrice competenze, piano, registri presenze, test awareness	Da completare	E09
Fornitori	Registro e valutazione fornitori critici, clausole security	Da completare	E10
Feedback/reclami	Registro feedback/reclami o dichiarazione assenza reclami	Da completare	E11
SGSI risk assessment	Criteri, valutazione, trattamento e stato attuazione controlli	Da completare	E12
SoA e rischi residui	SoA completa Annex A e approvazione rischi residui	Da completare	E13
Incidenti	Procedura e registro incidenti / dichiarazione nessun incidente	Da completare	E14
Continuita ICT	BCP/prontezza ICT e test	Da completare	E14
Accessi	Policy accessi e registro utenze	Da completare	E14
Backup	Piano backup, log e test restore	Da completare	E14

Chiusura fascicolo

Ruolo	Nome	Firma	Data
CEO / Top Management	Giorgio Garrafa	_____	____ / ____ / _____
Responsabile sistema integrato	_____	_____	____ / ____ / _____
Responsabile IT / tecnico	_____	_____	____ / ____ / _____

Fine documento