GESAN S.r.l.

Dossier Evidenze ISO/IEC 27001:2022

Audit di sorveglianza - Stage di vigilanza

Versione enterprise integrata con visura, mansionario aziendale, organigramma funzionale, immagini e mappatura persone - mansioni - asset - rischi - controlli - evidenze.

Campo	Valore
Organizzazione	GESAN S.r.l.
Sistema di gestione	ISO/IEC 27001:2022 - Information Security Management System
Finalita del documento	Preparazione senior enterprise allo stage di vigilanza: evidenze documentali, operative, tecniche, organizzative e di responsabilita.
Integrazioni V2	Allegato 2 Mansionario aziendale; Allegato 3 Organigramma funzionale; immagini documentali; collegamento nominativo tra funzioni, mansioni, asset, rischi, controlli ed evidenze.
Perimetro richiamato	Servizi ICT sanitari, sviluppo software, data center, hosting, sistemi clinici, supporto, help desk, call/contact center, R&S e processi di governo del SGSI.
Periodo evidenze consigliato	Dalla precedente verifica al giorno dell audit, con focus sugli ultimi 12 mesi.
Classificazione	Riservato - Uso interno
Data documento	05/05/2026

Executive note: questo dossier e concepito per essere usato come audit room index e come matrice di difesa del SGSI. Le tabelle non sostituiscono nomine, log, ticket, report tecnici o registrazioni reali: indicano cosa l auditor dovrebbe poter vedere, come collegarlo al rischio e quale ownership dimostrare.

Indice

1. Fonti, integrazione documentale e criteri di lettura

La presente versione integra i documenti aziendali allegati e li trasforma in evidenze operative per la sorveglianza ISO/IEC 27001. Il criterio consulenziale adottato non e meramente documentale: ogni informazione organizzativa viene collegata a responsabilita, asset informativi, scenari di rischio, controlli applicabili e prove da fornire all auditor.

La logica di audit proposta e: 1) dimostrare il perimetro; 2) dimostrare che le responsabilita sono assegnate; 3) dimostrare che gli asset sono noti e controllati; 4) dimostrare che i rischi sono valutati; 5) dimostrare che controlli e registrazioni sono attivi nel periodo di sorveglianza.

Fonte integrata	Informazione estratta	Impatto sul dossier
Visura camerale GESAN S.r.l.	Unita locali in San Nicola La Strada, attivita ICT, software, hosting, elaborazione dati, call center, R&S, manutenzione informatica; addetti medi rilevati.	Conferma perimetro fisico-operativo, processi, ATECO, sedi, asset e tipologia di servizi da coprire nel SGSI.
Allegato 2 - Mansionario aziendale	Ruoli e mansioni: DGE, RD, REG-UE, RSGQ, RSPP, PROD, MAG, AMM, COM, ACQ, SER, DT.	Base per collegare responsabilita organizzative, competenze, documenti da produrre, processi e controlli ISO 27001.
Allegato 3 - Organigramma funzionale	Nominativi, funzioni aziendali, linee di riporto e aree operative: CEO, General Manager, amministrazione, qualita, tecnica, sistemistica/sicurezza, team applicativi, assistenza, help desk, call center, commerciale, R&S.	Base per mappare persone/funzioni con asset, rischi, owner e intervistati in audit.
Sito istituzionale GESAN	Health care software, software factory, call center, data center, R&S, prodotti digital health, telemedicina, sistemi clinici, RIS/PACS/LIS, cartella clinica e soluzioni di accoglienza.	Contestualizzazione esterna e tecnica del perimetro SGSI e delle aspettative dei clienti sanitari.

1.1 Criterio di collegamento mansioni - asset - rischi

Per ogni persona/funzione viene applicata una matrice di tracciabilita che deve essere dimostrabile in audit con evidenze effettive. La catena minima e: funzione organizzativa -> mansione/profilo autorizzativo -> asset trattati -> rischio associato -> controllo applicato -> registrazione oggettiva.

Elemento	Domanda dell auditor	Evidenza senior da predisporre
Funzione e mansione	Chi e responsabile del processo? La mansione e coerente con l organigramma?	Organigramma firmato e aggiornato; mansionario; nomine; job description; deleghe; RACI SGSI.
Asset	Quali asset informativi sono gestiti dalla funzione?	Inventario asset con owner; classificazione CIA; elenco applicazioni, server, database, postazioni, repository, ticketing, contratti.
Rischio	Quali rischi derivano dal ruolo e dagli asset gestiti?	Risk assessment; risk treatment plan; accettazioni; risk owner; correlazione con incidenti, vulnerabilita, audit e cambiamenti.
Controllo	Quali controlli riducono il rischio?	SoA aggiornata; procedure; configurazioni tecniche; policy accessi; logging; backup; formazione; review periodiche.
Registrazione	Il controllo e stato realmente eseguito nel periodo?	Ticket, log, verbali, report, estrazioni accessi, evidenze di restore, scan vulnerabilita, audit interni, riesame direzione.

2. Evidenze visuali integrate dai documenti allegati

Le immagini riportate di seguito devono essere usate in audit come evidenze di contesto, non come unica prova. La prova completa e data dalla combinazione di documento originale, stato di revisione, firma/approvazione, registro distribuzione, coerenza con interviste e registrazioni operative.

2.1 Organigramma funzionale

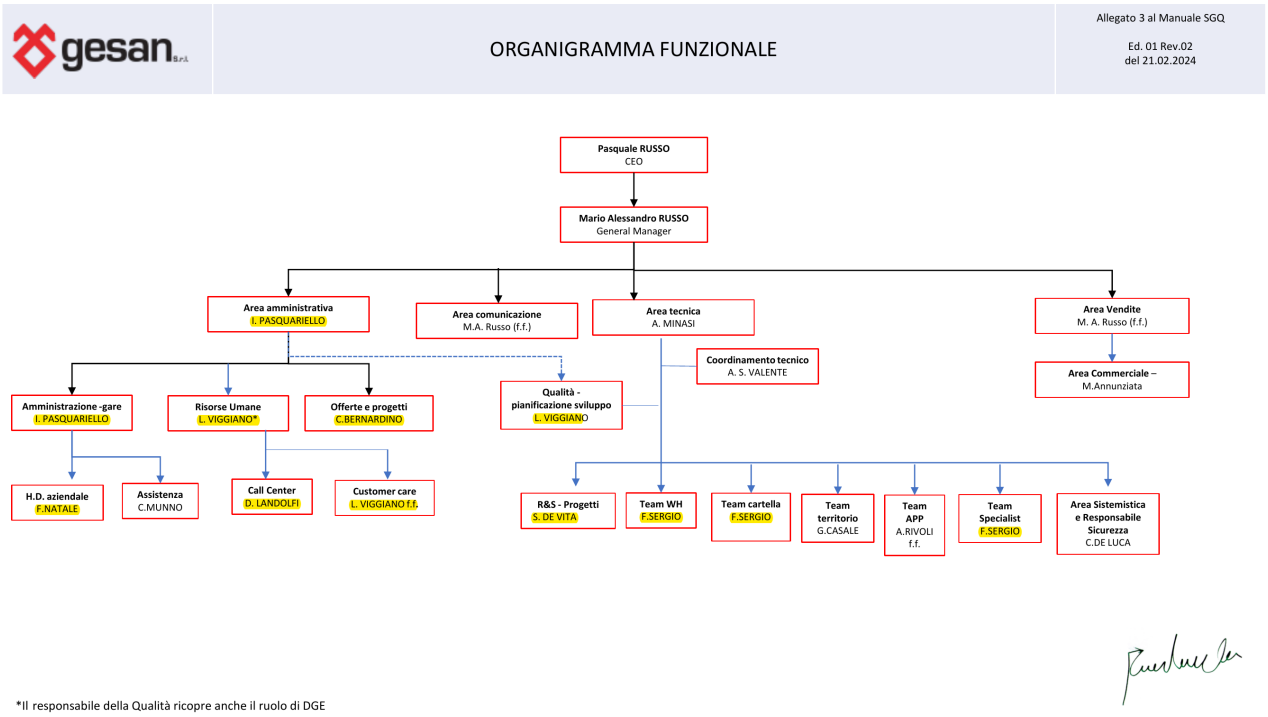


Figura 1 - Organigramma funzionale GESAN, Allegato 3 al Manuale SGQ, Ed. 01 Rev.02 del 21.02.2024. Da utilizzare per individuare intervistati, owner dei processi e coerenza tra mansioni, accessi, asset e rischi.

2.2 Mansionario aziendale - frontespizio e ruoli

gesan S.r.l.	**MANSIONARIO AZIENDALE**	**Allegato 2 al Manuale SGQ** **Ed. 01 Rev.00** del 24.10.2022

INDICE

Figura 2 - Mansionario aziendale, Allegato 2 al Manuale SGQ, Ed. 01 Rev.00 del 24.10.2022. Il documento elenca ruoli direzionali, qualita, amministrazione, commerciale, acquisti, installazione/manutenzione e direzione tecnica.

2.3 Visura camerale - attivita, addetti e unita locali

Registro Imprese
Archivio ufficiale della CCIAA
Documento n . A CA2MCFPT0N6D150689B5
estratto dal Registro Imprese in data 05/05/2026

GESAN S.R.L.
Codice Fiscale 06693080639

Addetti nel comune di SAN NICOLA LA STRADA (CE)
Unità locali: 7

	I trimestre	II trimestre	III trimestre	IV trimestre	Valore medio
Dipendenti	66	68	67	66	67
Indipendenti	0	0	0	0	0
Totale	66	68	67	66	67

5 Sedi secondarie ed unita' locali

Unita' Locale n. CE/7	VIA TORINO 14 SAN NICOLA LA STRADA (CE) CAP 81020
Unita' Locale n. CE/8	VIA ANTONIO PACINOTTI SNC SAN NICOLA LA STRADA (CE) CAP 81020

Unita' Locale n. CE/7

Sede Operativa
Data apertura: 16/01/2024

Indirizzo
SAN NICOLA LA STRADA (CE)
VIA TORINO 14 CAP 81020

Attivita' esercitata
IL 24/01/1997 ATTIVITA ESERCITATA DALL'IMPRESA :SERVIZI DI TELEMATICA,ROBOTICA,EIDOMATICA
IL 05/12/2003 E' INIZIATA L' ATTIVITA' DI RICERCA NELL'AMBITO DELL'ORGANIZZAZIONE SANITARIA
18/04/2006 CONSULENZA PER INSTALLAZIONE DI SISTEMI INFORMATICI E HARDWARE
EDIZIONI SOFTWARE
ALTRE REALIZZAZIONI DI SOFTWARE E CONSULENZA INFORMATICA
ELABORAZIONE ELETTRONICA DEI DATI
BANCHE DI DATI
MANUTENZIONE E RIPARAZIONE DI MACCHINE PER UFFICIO,APPARECCHIATURE E MATERIALE INFORMATICO.
ATTIVITA DEI CALL CENTER

Classificazione ATECO 2025 dell'attività
Codice: 62.90.09 - altre attività dei servizi connessi alle tecnologie dell'informazione e dell'informatica n.c.a.
Importanza: primaria Registro Imprese

Codice: 33.12.51 - riparazione e manutenzione di macchine e attrezzature per ufficio
Importanza: secondaria Registro Imprese

Codice: 58.29.00 - edizione di altri software
Importanza: secondaria Registro Imprese

Codice: 62.20.10 - attività di consulenza informatica
Importanza: secondaria Registro Imprese

Codice: 63.10.10 - fornitura di infrastrutture informatiche, hosting e attività connesse
Importanza: secondaria Registro Imprese

Codice: 63.10.2 - elaborazione dati
Importanza: secondaria Registro Imprese

Codice: 72.10 - ricerca e sviluppo sperimentale nel campo delle scienze naturali e dell'ingegneria
Importanza: secondaria Registro Imprese

Codice: 82.20.00 - attività dei call center
Importanza: secondaria Registro Imprese

Codice: 95.10.10 - riparazione e manutenzione di computer e periferiche
Importanza: secondaria Registro Imprese

Visura ordinaria di unita' locale o sede secondaria • **3** di **4**

Figura 3 - Estratto visura: addetti nel Comune di San Nicola La Strada, unita locali e attivita esercitate. Rilevante per perimetro fisico, processi ICT, call center, elaborazione dati, hosting, R&S; e manutenzione informatica.

2.4 Evidenza visuale sito istituzionale - quadro 1

page-01.png


GESAN S.r.l.

Dossier evidenze ISO/IEC 27001:2022

Audit di sorveglianza - Stage di vigilanza

page-02.png


Indice

page-03.png

page-04.png

page-05.png


1. Premessa, finalita e approccio di audit

page-06.png


2. Profilo GESAN e implicazioni per la sorveglianza ISO 27001

page-07.png


3. Governance del pacchetto evidenze

page-08.png

page-09.png

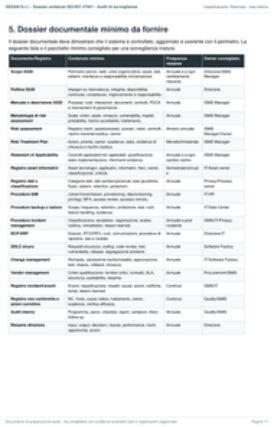

4. Evidenze obbligatorie per clausole ISO/IEC 27001

Figura - Ricognizione visuale del sito istituzionale GESAN: contenuti usati per contestualizzare servizi, prodotti digital health, data center, software factory, call/contact center e aree applicative.

2.5 Evidenza visuale sito istituzionale - quadro 2

page-10.png

page-11.png



page-12.png

page-13.png

page-14.png

page-15.png

page-16.png

page-17.png

page-18.png

Figura - Ricognizione visuale del sito istituzionale GESAN: contenuti usati per contestualizzare servizi, prodotti digital health, data center, software factory, call/contact center e aree applicative.

2.6 Evidenza visuale sito istituzionale - quadro 3

page-19.png

page-20.png

page-21.png

page-22.png

page-23.png

page-24.png

page-25.png

page-26.png

page-27.png

Figura - Ricognizione visuale del sito istituzionale GESAN: contenuti usati per contestualizzare servizi, prodotti digital health, data center, software factory, call/contact center e aree applicative.

3. Mappa nominativa: dipendenti/funzioni, mansioni, asset, rischi ed evidenze

La tabella seguente costituisce la matrice principale richiesta per la sorveglianza. Essa collega i nominativi/funzioni riportati nell organigramma con le mansioni richiamate dal mansionario aziendale e con asset, rischi, controlli ed evidenze da rendere disponibili. Dove il documento non assegna formalmente una mansione ISO 27001 nominativa, il collegamento e indicato come proposta di raccordo da validare con nomine interne o verbale di Direzione.

Dipendente / funzione	Ruolo da organigramma	Raccordo mansionario/SGSI	Asset principali	Rischi principali	Evidenze chiave
Pasquale Russo	CEO	Alta Direzione / DGE / risk acceptance	Politiche, obiettivi, budget, contratti strategici, reputazione, perimetro SGSI	Mancato commitment, risorse insufficienti, rischi non accettati formalmente, obiettivi non monitorati	Politica SGSI firmata; riesame direzione; approvazione rischio residuo; piano obiettivi; allocazione risorse
Mario Alessandro Russo	General Manager; Area Vendite f.f.; Area Comunicazione f.f.	DGE/RD/COM; governo operativo e contrattuale	Portafoglio clienti, offerte, comunicazioni, contratti, SLA, priorita operative	Impegni contrattuali non allineati a sicurezza, comunicazioni non autorizzate, requisiti cliente non tradotti in controlli	Riesame requisiti contrattuali; approvazione offerte; clausole sicurezza; piano comunicazione; tracciamento richieste cliente
I. Pasquariello	Area amministrativa; Amministrazione gare	AMM / supporto gare e documenti amministrativi	Dati contabili, fatture, scadenziari, gare, documentazione amministrativa, dati fornitori	Esposizione dati amministrativi, errori di archiviazione, accessi impropri a documenti di gara, frodi documentali	Registro accessi cartelle amministrative; segregazione ruoli; procedure gare; backup documentale; approvazioni; conservazione
L. Viggiano	Risorse Umane; Qualita - pianificazione sviluppo; Customer care f.f.	RSGQ / HR / DGE se confermato dal ruolo qualita	Documenti SGSI/SGQ, audit, formazione, competenze, customer care, piani sviluppo	Documenti obsoleti, personale non formato, offboarding incompleto, reclami non analizzati, azioni correttive non efficaci	Registro documenti; piano audit; verbali NC/AC; matrice competenze; formazione security; onboarding/offboarding; customer feedback
C. De Luca	Area sistemistica e Responsabile Sicurezza	Responsabile Sicurezza / DT / SER tecnologico	Data center, server, rete, firewall, VPN, backup, log, account privilegiati, DB, monitoraggio	Ransomware, indisponibilita servizi sanitari, accessi privilegiati abusivi, perdita backup, configurazioni deboli	Inventario sistemi; hardening; MFA; access review; backup/restore; vulnerability scan; patch report; log review; incident register
A. Minasi	Area tecnica	DT / coordinamento tecnico operativo	Architetture applicative, ambienti progetto, procedure tecniche, documentazione sistemi, rilascio software	Progettazione insicura, modifiche non controllate, scarsa separazione ambienti, errori di configurazione	Change management; disegni architetturali; test plan; release notes; segregation dev/test/prod; technical review
A. S. Valente	Coordinamento tecnico	DT / SER / coordinamento commesse	Piani tecnici, ticket, commesse, interventi, calendari, risorse tecniche	SLA non rispettati, interventi non autorizzati, tracciabilita incompleta, escalation tardive	Piano commesse; ticket campione; verbali riunioni tecniche; autorizzazioni intervento; report SLA; escalation log
S. De Vita	R&S - Progetti	R&D / DT / gestione progetti innovativi	Prototipi, dati progetto, repository R&D, know-how, documenti partner/universita	Perdita IP, condivisione incontrollata di dati, prototipi non sicuri, requisiti privacy non considerati	NDA; registro progetti; classificazione dati; accessi repository; privacy/security by design; deliverable e verbali
F. Sergio	Team WH; Team cartella; Team Specialist	Owner applicativo / sviluppo software	Web Hospital, cartella clinica, moduli specialistici, codice, repository, database applicativi	Vulnerabilita software, errori su dati clinici, mancata integrita applicativa, accessi eccessivi a dati sanitari	Secure SDLC; code review; test sicurezza; tracciamento commit; release approval; segregazione ambienti; remediation bug
G. Casale	Team territorio	Owner applicativo medicina territoriale	Sistemi territoriali, telemedicina, integrazioni MMG/PLS, dati paziente, workflow assistenziali	Accesso remoto non controllato, indisponibilita piattaforma, errata gestione consensi/dati sanitari	RBAC; audit log; test integrazioni; cifratura; disponibilita servizio; DPIA/valutazioni privacy ove applicabili
A. Rivoli	Team APP f.f.	Owner applicativo web/mobile/API	Applicazioni, API, front-end/back-end, credenziali tecniche, ambienti mobile/web	API esposte, sessioni deboli, storage non sicuro, mancato controllo rilasci	API security; secrets management; test OWASP; release checklist; gestione versioni; monitoring applicativo
F. Natale	H.D. aziendale	Help desk / supporto utenti	Ticket, richieste accesso, reset password, endpoint, richieste utenti, knowledge base	Social engineering, reset non autorizzati, escalation errate, ticket con dati sensibili	Procedura identificazione utente; ticketing; approvazioni accessi; masking dati; training phishing; audit ticket
C. Munno	Assistenza	SER / assistenza applicativa e manutenzione	Accessi remoti cliente, ticket supporto, configurazioni applicative, log intervento, dati cliente	Accesso non autorizzato a sistemi cliente, modifiche non tracciate, esposizione dati durante assistenza	Autorizzazione cliente; session logging; ticket chiuso con evidenza; MFA/VPN; segregazione privilegi; report intervento

Dipendente / funzione	Ruolo da organigramma	Raccordo mansionario/SGSI	Asset principali	Rischi principali	Evidenze chiave
D. Landolfi	Call Center	Responsabile call/contact center	Piattaforme call center, CRM, script, registrazioni, anagrafiche, eventuali dati sanitari/servizio	Divulgazione dati, identificazione utente debole, retention non controllata, operatori non formati	Script identificazione; formazione privacy/security; accessi profilati; retention registrazioni; clean desk; monitoraggio qualita
M. Annunziata	Area Commerciale	COM / gestione clienti e trattative	CRM, contatti clienti, offerte, contratti, NDA, pipeline commerciale	Fuga informazioni commerciali, requisiti sicurezza non formalizzati, contratti senza clausole data protection	Riesame offerte; NDA; template clausole sicurezza; archivio protetto; accessi CRM; gestione reclami
C. Bernardino	Offerte e progetti	COM / project pre-sales / requisiti	Offerte tecniche, capitolati, documentazione progetto, richieste cliente, requisiti sicurezza	Requisiti di sicurezza omessi, stime errate, documenti cliente gestiti senza classificazione	Checklist offerta; security requirements; approvazione tecnica; versioning; archiviazione controllata

4. Schede senior per funzione: responsabilita, asset, rischi, controlli e campioni audit

Le schede seguenti devono essere usate per preparare interviste, campionamenti e raccolta evidenze. Ogni scheda identifica la linea di difesa attesa in audit e i documenti da avere pronti.

Pasquale Russo - CEO

Dimostrare leadership, indirizzo strategico, risk appetite, disponibilita risorse e approvazione delle decisioni rilevanti per il SGSI.

Dimensione	Contenuto operativo
Asset	Politica SGSI, scopo, obiettivi, budget sicurezza, contratti strategici, reputazione aziendale, decisioni di rischio residuo.
Rischi	SGSI percepito come adempimento formale; rischio residuo non approvato; carenza risorse; mancata prioritizzazione delle azioni correttive; incoerenza tra strategia commerciale e sicurezza.
Controlli attesi	Riesame della Direzione; approvazione risk treatment; obiettivi misurabili; assegnazione risorse; verifica KPI; escalation incidenti rilevanti.
Evidenze da mostrare	Politica SGSI firmata; verbale riesame Direzione; registro decisioni; approvazione risk assessment e SoA; piano obiettivi; budget/capitoli investimento; comunicazioni interne.
Domande probabili	Quali sono i principali rischi informativi aziendali?; Quali risultati SGSI sono stati riesaminati?; Quali risorse sono state stanziate dopo audit/incidenti/cambiamenti?

Mario Alessandro Russo - General Manager / vendite e comunicazione f.f.

Presidiare allineamento tra strategia operativa, requisiti cliente, SLA, comunicazioni esterne e impegni contrattuali di sicurezza.

Dimensione	Contenuto operativo
Asset	Contratti, offerte, SLA, clienti strategici, comunicazioni istituzionali, pipeline commerciale, informazioni riservate di progetto.
Rischi	Accettazione di SLA non sostenibili; clausole di sicurezza non presidiate; diffusione di informazioni non autorizzate; cambiamenti contrattuali non comunicati ai team tecnici.
Controlli attesi	Riesame requisiti cliente; approvazione offerte; clausole sicurezza/privacy; processo comunicazioni; coinvolgimento responsabile sicurezza in offerte critiche.
Evidenze da mostrare	Campioni offerte; contratti con clausole sicurezza; verbali kick-off; registro comunicazioni; evidenze di escalation requisiti; approvazioni di progetto.
Domande probabili	Come vengono recepiti i requisiti di sicurezza nei contratti?; Chi approva impegni su SLA e continuita?; Come vengono gestite comunicazioni in caso di incidente?

L. Viggiano - Qualita, pianificazione sviluppo, HR, customer care f.f.

Garantire governo documentale, audit interni, competenza, formazione, customer feedback e integrazione tra SGQ e SGSI.

Dimensione	Contenuto operativo
Asset	Manuali, procedure, registri formazione, audit, NC/AC, piano sviluppo, customer feedback, documentazione HR.
Rischi	Documenti obsoleti; formazione non tracciata; personale con accessi non coerenti al ruolo; reclami non analizzati; NC non chiuse.
Controlli attesi	Document control; training plan; internal audit; corrective actions; competenze e consapevolezza; onboarding/offboarding con IT/security.
Evidenze da mostrare	Registro documenti; piano audit; report audit interno; azioni correttive; registro formazione; matrice competenze; campioni di presa visione policy; customer satisfaction.
Domande probabili	Come viene garantito che il personale conosca le policy?; Come sono monitorate le azioni correttive?; Come si collega offboarding HR a rimozione accessi IT?

C. De Luca - Area Sistemistica e Responsabile Sicurezza

Presidiare controlli tecnologici, sicurezza infrastrutturale, accessi privilegiati, disponibilita, backup, logging, vulnerabilita e incidenti.

Dimensione	Contenuto operativo
Asset	Data center, server, apparati rete, firewall, VPN, EDR/antivirus, log, backup, account admin, database, monitoraggio, infrastrutture cliente gestite.
Rischi	Ransomware; downtime servizi sanitari; compromissione credenziali privilegiate; mancato restore; vulnerabilita critiche non trattate; log insufficienti.
Controlli attesi	MFA; least privilege; backup e restore test; patch/vulnerability management; hardening; segregazione rete; monitoraggio log; incident response.
Evidenze da mostrare	Inventario asset; estratti access review; elenco admin; log MFA/VPN; report backup e restore; scan vulnerabilita; patch report; incident register; configurazioni firewall campione.

Dimensione	Contenuto operativo
Domande probabili	Quali asset critici sono monitorati?; Quando e stato effettuato l ultimo restore test?; Come vengono gestite vulnerabilita critiche?; Come sono controllati gli account privilegiati?

A. Minasi - Area Tecnica

Assicurare governo tecnico di architetture, configurazioni, modifiche, ambienti e integrazione tra sviluppo, sistemi e assistenza.

Dimensione	Contenuto operativo
Asset	Architetture, ambienti dev/test/prod, specifiche tecniche, configurazioni, change, release, documentazione cliente.
Rischi	Modifiche non approvate; ambienti non segregati; configurazioni deboli; impatti non valutati su disponibilita e integrita dati.
Controlli attesi	Change advisory; segregation of environments; review tecnica; checklist rilascio; approvazione configurazioni; test non regressione.
Evidenze da mostrare	Registro change; campioni release notes; approvazioni tecniche; diagrammi architettura; test report; rollback plan; autorizzazioni accessi tecnici.
Domande probabili	Come si approva una modifica critica?; Come si dimostra la separazione dev/test/prod?; Quali controlli impediscono modifiche dirette in produzione?

A. S. Valente - Coordinamento tecnico

Coordinare commesse, interventi tecnici, risorse specialistiche, priorita, SLA, escalation e tracciamento operativo.

Dimensione	Contenuto operativo
Asset	Piani commessa, ticket, calendari intervento, documentazione installazione, report SLA, autorizzazioni cliente.
Rischi	Interventi non tracciati; ritardi SLA; attivita non autorizzate presso cliente; scarsa escalation incidenti.
Controlli attesi	Ticketing obbligatorio; autorizzazione interventi; SLA monitoring; escalation matrix; chiusura ticket con evidenza; riunioni tecniche.
Evidenze da mostrare	Ticket campionati; piano interventi; report SLA; verbali riunioni; autorizzazioni cliente; report tecnico post intervento.
Domande probabili	Come viene garantita la tracciabilita degli interventi?; Come si distinguono richieste ordinarie e incidenti di sicurezza?

S. De Vita - R&S Progetti

Proteggere know-how, prototipi, dati progettuali e collaborazioni di ricerca, integrando security/privacy by design nei progetti innovativi.

Dimensione	Contenuto operativo
Asset	Progetti R&S, prototipi, repository, dati di test, documenti partner, deliverable, proprieta intellettuale.
Rischi	Esfiltrazione IP; uso dati reali non anonimizzati; accessi partner non controllati; prototipi con sicurezza non verificata.
Controlli attesi	Classificazione informazioni; NDA; accessi repository; pseudonimizzazione/anonimizzazione; review privacy/security; controllo versioni.
Evidenze da mostrare	Elenco progetti; NDA; matrice accessi; documenti di progetto; registro dati usati; valutazioni privacy; log repository; verbali partner.
Domande probabili	I progetti usano dati reali o sintetici?; Come vengono controllati accessi di partner e ricercatori?; Quando viene eseguita la security review?

F. Sergio - Team WH / Team cartella / Team Specialist

Presidiare sicurezza applicativa, integrita dati clinici, gestione codice, rilasci e manutenzione di applicazioni sanitarie critiche.

Dimensione	Contenuto operativo
Asset	Web Hospital, cartella clinica, moduli specialistici, source code, repository, DB applicativi, configurazioni applicative.
Rischi	Bug su dati clinici; vulnerabilita web; data leakage; codice non revisionato; rilasci non testati; credenziali hardcoded.
Controlli attesi	Secure coding; code review; SAST/DAST ove disponibile; branch protection; test plan; segregation duties; secrets management; release approval.
Evidenze da mostrare	Commit e pull request campione; test report; checklist sicurezza; release notes; bug remediation; accessi repository; approvazioni deploy.
Domande probabili	Come viene documentata la revisione codice?; Quali test sono svolti prima del rilascio?; Come vengono gestiti bug su dati clinici?

G. Casale - Team territorio

Garantire sicurezza e disponibilita dei servizi territoriali, telemedicina e integrazioni verso medici, pazienti e strutture esterne.

Dimensione	Contenuto operativo
Asset	Piattaforme territoriali, telemedicina, integrazioni, API, dati paziente, consensi, workflow assistenziali.
Rischi	Accesso remoto improprio; indisponibilita servizi; errata integrazione con sistemi esterni; mancata protezione dati particolari.
Controlli attesi	RBAC; API authentication; logging accessi; monitoraggio disponibilita; cifratura; gestione consensi; incident escalation.
Evidenze da mostrare	Matrice ruoli applicativi; log accessi; monitoraggio uptime; test API; registro anomalie; valutazioni privacy; ticket integrazione.
Domande probabili	Come si controllano utenti esterni?; Come si tracciano accessi ai dati del paziente?; Quali SLA sono applicabili?

A. Rivoli - Team APP f.f.

Presidiare sicurezza di applicazioni, interfacce web/mobile, API e componenti front-end/back-end.

Dimensione	Contenuto operativo
Asset	APP, API, front-end, back-end, chiavi di integrazione, ambienti di build, pipeline, store/release package.
Rischi	API abuse; token/sessioni gestiti in modo debole; secrets nel codice; dipendenze vulnerabili; rilascio non autorizzato.
Controlli attesi	OWASP checklist; dependency scanning; API gateway/auth; secrets vault; approval release; test sicurezza mobile/web; logging applicativo.
Evidenze da mostrare	Distinta versioni; pipeline log; vulnerability/dependency report; checklist OWASP; release approval; evidenze test; gestione segreti.
Domande probabili	Come vengono gestite chiavi API?; Quali controlli impediscono deploy non autorizzati?; Come vengono tracciate vulnerabilita di librerie?

F. Natale - H.D. aziendale

Gestire richieste utenti e supporto interno garantendo identificazione, autorizzazione, tracciabilita e protezione delle informazioni nei ticket.

Dimensione	Contenuto operativo
Asset	Ticket, richieste accesso, reset password, endpoint, knowledge base, procedure supporto, dati utente.
Rischi	Social engineering; reset password non autorizzato; dati sensibili nei ticket; escalation errata; accessi non rimossi.
Controlli attesi	Identity verification; workflow approvazione accessi; masking dati; categorizzazione incidenti; training operatori; access review.
Evidenze da mostrare	Ticket campione reset/accessi; procedura help desk; log approvazioni; registro escalation; formazione phishing; report SLA help desk.
Domande probabili	Come verificate l identita dell utente?; Quando un ticket diventa incidente di sicurezza?; Come vengono protetti dati nei ticket?

C. Munno - Assistenza

Erogare assistenza applicativa e manutentiva presso clienti, garantendo autorizzazioni, tracciabilita, controllo accessi remoti e minimizzazione dati.

Dimensione	Contenuto operativo
Asset	Accessi remoti, sessioni assistenza, ticket cliente, configurazioni applicative, log intervento, dati cliente.
Rischi	Accesso non autorizzato; attivita non tracciata; errore in ambiente cliente; copia non autorizzata di dati; credenziali condivise.
Controlli attesi	Remote access policy; MFA/VPN; autorizzazione cliente; session log; ticketing; divieto credenziali condivise; chiusura intervento validata.
Evidenze da mostrare	Log VPN; ticket intervento; autorizzazioni cliente; report assistenza; elenco account assistenza; access review; training privacy.
Domande probabili	Come viene autorizzata una sessione remota?; Sono usati account nominativi?; Quali dati possono essere copiati in assistenza?

D. Landolfi - Call Center

Garantire gestione sicura di contatti, conversazioni, anagrafiche, script e possibili dati sanitari/amministrativi trattati dagli operatori.

Dimensione	Contenuto operativo
Asset	Piattaforma call center, CRM, script, registrazioni, anagrafiche, code chiamata, report qualita.
Rischi	Divulgazione dati; identificazione chiamante insufficiente; retention eccessiva registrazioni; stampa o annotazione non autorizzata; training insufficiente.
Controlli attesi	Script di identificazione; profili utente; clean desk/screen; formazione privacy; retention; monitoraggio qualita; procedure escalation.

Dimensione	Contenuto operativo
Evidenze da mostrare	Script approvati; profili operatori; registro formazione; campioni ticket/chiamate anonimizzati; policy retention; report qualita; audit postazioni.
Domande probabili	Come identificate l utente?; Quali informazioni possono essere comunicate telefonicamente?; Quanto vengono conservate eventuali registrazioni?

M. Annunziata / C. Bernardino - Commerciale, offerte e progetti

Garantire che requisiti cliente, offerte, gare e progetti includano obblighi di sicurezza, privacy, continuita, SLA e responsabilita.

Dimensione	Contenuto operativo
Asset	CRM, offerte, capitolati, contratti, NDA, documenti gara, requisiti cliente, report di progetto.
Rischi	Requisiti di sicurezza non recepiti; perdita di documenti riservati; impegni contrattuali non sostenibili; dati personali in documenti commerciali.
Controlli attesi	Riesame offerta; checklist security/privacy; classificazione documenti; approvazioni; clausole contrattuali; archiviazione protetta.
Evidenze da mostrare	Offerte campione; checklist requisiti; clausole sicurezza; NDA; approvazioni DGE/GM/tecnico; registro varianti; template contrattuali.
Domande probabili	Chi valida requisiti di sicurezza in offerta?; Come vengono gestiti allegati tecnici riservati?; Come passano i requisiti al team tecnico?

5. Registro asset enterprise collegato alle funzioni

Il registro asset deve dimostrare che i beni informativi sono identificati, classificati, assegnati a owner e collegati ai rischi. Per la sorveglianza si suggerisce di presentare almeno le seguenti famiglie di asset, con estrazione aggiornata da CMDB, inventario software, inventario apparati, repository, sistema ticketing e registro documentale.

ID	Asset / famiglia	Owner	Contenuto	Classificazione CIA	Rischi	Evidenze minime
A-01	Data center e infrastrutture core	C. De Luca / Area sistemistica	Server, storage, rete, firewall, virtualizzazione, backup, monitoraggio	Riservatezza alta, Integrita alta, Disponibilita molto alta	Downtime, ransomware, guasto storage, errore configurazione	Asset inventory; schema rete; backup; restore; patch; log; DR/BCP
A-02	Applicazioni cliniche WH /cartella/specialistiche	F. Sergio / Area tecnica	Web Hospital, cartella clinica, moduli specialistici, DB applicativi	C-I-D molto alta per dati clinici	Vulnerabilita applicativa, alterazione dati clinici, errore rilascio	SDLC; test; release; code review; accessi applicativi; incidenti applicativi
A-03	Piattaforme territorio e telemedicina	G. Casale / Team territorio	Soluzioni territoriali, telemonitoraggio, integrazioni, consensi, API	C-I-D molto alta	Accesso remoto improprio, indisponibilita, errore integrazione	RBAC; log; API security; monitoraggio; valutazioni privacy; test integrazione
A-04	APP, API e componenti web/mobile	A. Rivoli / Team APP	Front-end, back-end, API, credenziali tecniche, librerie, pipeline	Alta	API abuse, vulnerabilita librerie, secrets nel codice	OWASP; dependency scan; secrets management; pipeline approval; test sicurezza
A-05	Repository codice e documentazione tecnica	A. Minasi / team applicativi	Source code, branch, issue tracker, release, documenti tecnici	C-I alta, D media	Leak codice, commit non revisionato, accessi non revocati	Access review repository; branch protection; commit log; code review; offboarding
A-06	Ticketing, help desk e assistenza clienti	F. Natale / C. Munno / A.S. Valente	Ticket, richieste accesso, incidenti, interventi, allegati cliente	Alta	Dati sensibili nei ticket, reset impropri, modifiche non autorizzate	Workflow approvativo; masking; SLA; categorizzazione incidenti; ticket campione
A-07	Call/contact center	D. Landolfi	Piattaforma chiamate, CRM, script, registrazioni, report qualita	Alta	Divulgazione dati, identificazione debole, retention non controllata	Script; profili operatori; training; retention; quality monitoring; clean desk
A-08	Documentazione SGSI/SGQ	L. Viggiano / RSGQ	Manuali, procedure, SoA, risk assessment, audit, NC/AC, riesami	Integrita alta, disponibilita alta	Documenti obsoleti, azioni non chiuse, evidenze incomplete	Registro documenti; distribuzione; versioning; audit; riesame; azioni correttive
A-09	Risorse umane e competenze	L. Viggiano / HR	Matrice competenze, formazione, contratti, onboarding/offboarding	Riservatezza alta	Personale non formato, accessi non revocati, competenze non dimostrate	Training plan; presenze; test; checklist onboarding/offboarding; job description
A-10	Amministrazione, gare e contratti	I. Pasquariello / C. Bernardino / M. Annunziata	Offerte, gare, fatture, contratti, NDA, scadenziari, documenti cliente	Alta	Fuga info, impegni non controllati, accessi impropri, frode documentale	Permessi; archiviazione protetta; template clausole; approvazioni; audit documentale
A-11	R&S, prototipi e proprieta intellettuale	S. De Vita	Progetti, prototipi, dataset, deliverable, repository R&D, partner	C-I alta	Perdita IP, dati test non anonimizzati, accessi partner deboli	NDA; classificazione; accessi; privacy by design; verbali progetto; log repository
A-12	Siti e ambienti cliente	C. Munno / A.S. Valente / C. De Luca	VPN, accessi remoti, installazioni, configurazioni, ambienti on premise/esterni	Alta	Accesso non autorizzato, responsabilita non chiare, tracciabilita incompleta	Contratti; autorizzazioni; log sessioni; ticket; nomine privacy; report intervento

6. Registro rischi SGSI collegato a persone, asset e controlli

Per lo stage di vigilanza e opportuno presentare un risk assessment vivo, con ownership effettiva. I rischi sotto riportati sono una base enterprise da integrare con probabilita, impatto, livello inerente, controlli esistenti, rischio residuo e stato del piano di trattamento.

ID	Scenario di rischio	Owner	Asset	Controlli chiave	Evidenze richieste
R-01	Ransomware su infrastruttura core	C. De Luca	A-01, A-02, A-03	EDR, backup immutabile/offline se presente, patching, segmentazione, least privilege, awareness	Restore test; report EDR; patch; access review; simulazione incidente
R-02	Compromissione account privilegiato	C. De Luca	A-01, A-12	MFA, PAM o registro admin, account nominativi, review periodica, logging	Lista admin; log MFA/VPN; estrazione SIEM; verbale access review
R-03	Errore di rilascio su applicazione clinica	F. Sergio / A. Minasi	A-02	Change management, test, approvazione release, rollback, segregazione ambienti	Change campione; test report; release note; rollback plan
R-04	Vulnerabilita web/API sfruttabile	A. Rivoli / F. Sergio	A-02, A-04	OWASP, code review, dependency scanning, test DAST/SAST, remediation	Scan vulnerabilita; backlog remediation; checklist OWASP; evidenze review
R-05	Perdita integrita dati clinici	F. Sergio / G. Casale	A-02, A-03	Controlli applicativi, audit trail, backup, test, permessi, validazioni DB	Audit log; test integrita; backup; permessi ruoli applicativi
R-06	Indisponibilita data center o servizio critico	C. De Luca / A.S. Valente	A-01, A-02, A-03	Monitoring, capacity, backup, DR/BCP, SLA, incident escalation	Uptime report; capacity report; test DR; incident log; SLA
R-07	Accesso remoto cliente non autorizzato	C. Munno / C. De Luca	A-12	VPN/MFA, account nominativi, autorizzazione cliente, session logging	Log VPN; ticket autorizzato; account list; report sessione
R-08	Data leakage da ticket/help desk	F. Natale / C. Munno	A-06	Masking, istruzioni ticket, limitazione allegati, ruoli, formazione	Ticket campione anonimizzati; procedura; formazione; review permessi
R-09	Divulgazione dati da call center	D. Landolfi	A-07	Script identificazione, training privacy, RBAC, retention, clean desk	Script; registro formazione; profili; audit postazione; retention policy
R-10	Offboarding incompleto	L. Viggiano / C. De Luca	A-05, A-09, A-12	Checklist HR-IT, disattivazione account, recupero asset, review post offboarding	Checklist offboarding; log disabilitazioni; access review; asset return
R-11	Fuga proprieta intellettuale R&S	S. De Vita	A-11	NDA, classificazione, accessi repository, data sharing policy	NDA; access matrix; log repository; verbali partner
R-12	Fornitore critico non governato	I. Pasquariello / C. De Luca / GM	A-01, A-10, A-12	Valutazione fornitori, clausole sicurezza, SLA, subfornitori, review	Vendor register; valutazioni; contratti; SLA; audit/attestazioni fornitore
R-13	Requisiti di sicurezza omessi in offerta/contratto	M. Annunziata / C. Bernardino / GM	A-10	Contract review, checklist sicurezza, coinvolgimento tecnico/security	Offerte campione; checklist; approvazioni; clausole
R-14	Documentazione SGSI non aggiornata	L. Viggiano	A-08	Document control, riesame periodico, distribuzione, audit interno	Registro documenti; revisioni; audit; lista distribuzione
R-15	Mancata consapevolezza personale	L. Viggiano / responsabili area	Tutti	Training annuale, phishing awareness, policy acknowledgement, onboarding	Piano formazione; presenze; test; presa visione policy
R-16	Log insufficienti per ricostruzione incidente	C. De Luca / owner applicativi	A-01-A-04	Logging standard, sincronizzazione oraria, retention, accesso log, review	Configurazioni log; NTP; retention; log sample; review periodica
R-17	Backup non ripristinabile	C. De Luca	A-01-A-03	Backup policy, monitoraggio job, test restore, separazione credenziali	Report backup; restore test; error log; piano remediation
R-18	Uso improprio dati reali in test/R&S	S. De Vita / F. Sergio / A. Rivoli	A-02-A-05-A-11	Data minimization, anonimizzazione, ambienti segregati, approvazioni	Registro dataset; evidenza anonimizzazione; accessi dev/test; policy test data

7. RACI SGSI per processi critici

La matrice RACI e una delle evidenze piu efficaci in sorveglianza: consente di dimostrare che non esistono aree grigie tra Direzione, qualita, sicurezza, sistemistica, sviluppo, supporto, commerciale e amministrazione.

Processo SGSI	A	R	C	I	Evidenza
Politica, scopo e obiettivi SGSI	CEO / GM	Qualita	Resp. Sicurezza, DT, Commerciale	Tutti responsabili area	Politica firmata; obiettivi; comunicazioni
Risk assessment e SoA	CEO / GM	Resp. Sicurezza + Qualita	DT, owner applicativi, HR, commerciale	Owner asset	Risk register; SoA; piano trattamento
Asset inventory	Resp. Sicurezza	Sistemistica + owner applicativi	Qualita, DT, help desk	Direzione	Inventario aggiornato; owner; classificazione
Gestione accessi e privilegi	Resp. Sicurezza	Sistemistica / Help Desk	HR, responsabili area	Direzione	Access review; richieste accesso; offboarding
Sviluppo sicuro e rilasci	DT / Area tecnica	Team applicativi	Sicurezza, Qualita, supporto	Clienti interessati	Change, test, release notes, code review
Backup, restore e continuita	Resp. Sicurezza	Sistemistica	DT, owner applicativi, Direzione	Clienti se previsto	Backup report; restore test; BCP/DR test
Incident management	Resp. Sicurezza	Sistemistica / Help desk / owner processo	Qualita, Direzione, DPO/privacy se presente	Clienti/autorita secondo caso	Incident register; RCA; comunicazioni; lessons learned
Audit interni e NC/AC	Qualita	Auditor interni / owner processo	Direzione, Responsabile Sicurezza	Responsabili area	Piano audit; report; azioni correttive
Fornitori critici	GM / Amministrazione	Acquisti / Sicurezza per requisiti IT	Commerciale, DT, Qualita	Owner asset	Vendor register; valutazioni; contratti
Formazione e consapevolezza	Direzione	HR / Qualita	Responsabile Sicurezza, responsabili area	Tutto personale	Piano formazione; presenze; test; onboarding
Call center e assistenza	GM / responsabili area	D. Landolfi / C. Munno / F. Natale	Sicurezza, Qualita, HR	Clienti e Direzione	Script; ticket; training; audit postazioni

8. Audit room index: evidenze da predisporre per clausole ISO/IEC 27001

La tabella seguente organizza le evidenze in una logica da audit room. Ogni evidenza deve essere versionata, datata, attribuita a un responsabile e collegata a un periodo di riferimento. L auditor deve poter seguire il filo: requisito -> rischio -> controllo -> registrazione.

Clausola	Evidenza enterprise	Owner primario	Campione atteso in sorveglianza
4.1 Contesto	Analisi contesto interno/esterno aggiornata; cambiamenti organizzativi, tecnologici, normativi e di mercato	Qualita / Direzione	Ultima revisione; evidenza di aggiornamento rispetto a organigramma, sedi, servizi e fornitori
4.2 Parti interessate	Matrice stakeholder e requisiti: clienti sanitari, pazienti/utenti, autorita, fornitori, dipendenti, auditor, partner R&S	Qualita / GM	Requisiti contrattuali e normativi recepiti nel risk assessment
4.3 Scopo SGSI	Scopo aggiornato con sedi, data center, ambienti, sviluppo software, call center, assistenza, R&S e siti cliente pertinenti	Direzione / Qualita	Coerenza tra scopo, visura, sito, organigramma, asset e SoA
4.4 SGSI	Process map SGSI e interazioni con SGQ, IT, sviluppo, assistenza, commerciale e HR	Qualita	Mappa processi, RACI, indicatori, registrazioni correnti
5.1 Leadership	Commitment Direzione, politica, obiettivi, risorse e decisioni di sicurezza	CEO / GM	Verbali, budget, comunicazioni, approvazioni rischio
5.2 Politica	Politica sicurezza informazioni approvata, comunicata e disponibile	Direzione / Qualita	Versione firmata; presa visione personale; pubblicazione interna
5.3 Ruoli e responsabilita	Organigramma, mansionario, nomine, RACI, owner asset/rischi	Direzione / Qualita	Mappatura nominativa V2; nomine responsabili; job description
6.1 Rischi e opportunita	Metodo risk assessment, registro rischi, trattamenti, accettazioni e opportunita di miglioramento	Resp. Sicurezza / Qualita	Campione di rischi alti, stato azioni, owner, scadenze
6.1.3 SoA	Dichiarazione di Applicabilita con motivazioni, controlli inclusi/esclusi, stato attuazione	Resp. Sicurezza / Qualita	SoA allineata ad Annex A:2022, audit interni, evidenze tecniche
6.2 Obiettivi	Obiettivi misurabili SGSI e KPI	Direzione / Qualita	Trend: access review, training, patching, backup, incidenti, vulnerabilita, SLA
7.1 Risorse	Risorse umane, tecniche, economiche e infrastrutturali per SGSI	Direzione	Budget, piani assunzione/formazione, contratti strumenti sicurezza
7.2 Competenza	Matrice competenze, formazione ruoli critici, qualifiche tecniche	HR / Qualita	Campione persone: sistemistica, sviluppo, call center, assistenza, help desk
7.3 Consapevolezza	Awareness security e privacy	Qualita / HR / Sicurezza	Presa visione policy, campagne phishing, test formazione
7.4 Comunicazione	Processo comunicazione interna/esterna e incident communication	GM / Qualita	Piano comunicazione, template incident, escalation
7.5 Informazioni documentate	Controllo documenti, versioni, distribuzione, archiviazione e protezione	Qualita	Registro documenti; versioni; permessi cartelle; backup documentale
8.1 Pianificazione operativa	Procedure operative per sviluppo, sistemi, assistenza, call center, change, incidenti, backup	Owner processo	Campioni esecuzione su ticket/log/report
8.2 Risk assessment periodico	Rivalutazione rischi dopo cambiamenti, incidenti, nuovi clienti/servizi	Resp. Sicurezza / Qualita	Risk review periodica; modifiche rispetto alla precedente sorveglianza
8.3 Risk treatment	Azioni di trattamento con responsabilita, scadenze e verifica efficacia	Owner rischio	Stato azioni; prove chiusura; rischio residuo aggiornato
9.1 Monitoraggio	KPI, misure tecniche, performance controlli, log review, SLA	Qualita / Sicurezza / owner	Dashboard KPI; trend; azioni correttive
9.2 Audit interno	Piano e report audit interno SGSI	Qualita / auditor interni	Audit eseguito prima della sorveglianza; NC e osservazioni chiuse o pianificate
9.3 Riesame Direzione	Riesame con input/output ISO 27001	CEO / GM / Qualita	Verbale completo, decisioni, risorse, miglioramenti, cambiamenti
10.1 Miglioramento	Registro miglioramenti, lessons learned, piani evolutivi	Qualita / Direzione	Azioni da audit, incidenti, vulnerabilita, clienti
10.2 Non conformita	NC, incidenti, reclami, RCA, correzioni e azioni correttive	Qualita / owner	Evidenza causa radice, azione, verifica efficacia

9. Mappatura Annex A: controlli e proprietari evidenze

La sorveglianza ISO/IEC 27001:2022 richiede coerenza tra SoA e implementazione reale. La seguente matrice non sostituisce la SoA ufficiale, ma indica i controlli che, per GESAN, appaiono maggiormente critici in base a servizi ICT sanitari, dati clinici, data center, sviluppo software, assistenza e call/contact center.

Dominio	Controllo/tema	Owner naturale	Evidenze senior
A.5 Organizzativi	Politiche, ruoli, segregazione, contatti autorita, threat intelligence, sicurezza progetti, inventario informazioni, acceptable use, restituzione asset, classificazione, supplier security, incident management, ICT readiness for business continuity	Direzione, Qualita, Sicurezza, owner processi	Policy; RACI; asset register; supplier register; incident register; BCP/DR; classification scheme; contratti
A.6 Persone	Screening, termini contrattuali, awareness, disciplina, termination, confidentiality, remote working, reporting security events	HR, Qualita, Sicurezza, responsabili area	Contratti/NDA; formazione; onboarding/offboarding; policy remote working; canali segnalazione; registro eventi
A.7 Fisici	Perimetro fisico, accessi fisici, sicurezza uffici, protezione da minacce fisiche, secure disposal/re-use, equipment security	Sistemistica, Direzione, amministrazione/sedi	Registro accessi data center/uffici; autorizzazioni; inventario asset fisici; smaltimento; controlli ambientali
A.8 Tecnologici	Endpoint, privilegi, access restriction, source code, authentication, capacity, malware, vulnerabilities, configuration, deletion, masking, DLP, backups, logging, monitoring, clock sync, network security, web filtering, cryptography, secure SDLC, test, change, data leakage, cloud services	Responsabile Sicurezza, sistemistica, team sviluppo, help desk	Hardening; EDR; MFA; access review; repo access; vulnerability scan; backup/restore; log review; SDLC; change; cloud register

9.1 Evidenze tecnologiche prioritarie da chiedere a C. De Luca / Area Sistemistica

Area tecnica	Evidenze minime	Criterio di accettazione auditor
Inventario infrastrutturale	Server, VM, apparati, firewall, backup, DB, sistemi monitorati, owner e criticita	Completo, aggiornato, coerente con scopo e data center; asset critici classificati.
Accessi privilegiati	Elenco admin, gruppi, policy password/MFA, log accessi, review semestrale	Account nominativi; privilegi giustificati; revoche documentate; MFA attivo sui sistemi critici.
Backup/restore	Policy, job report, errori, test restore, RPO/RTO, supporti/immutabilita	Almeno un restore test recente sui sistemi critici; anomalie gestite con ticket.
Vulnerability/patch	Report scan, patch compliance, remediation, eccezioni motivate	Vulnerabilita critiche trattate entro SLA interno o con risk acceptance.
Logging/monitoraggio	Fonti log, retention, alert, review periodica, time sync	Log sufficienti a ricostruire accessi e incidenti; eventi critici presidiati.
Network/security	Schema rete, segmentazione, VPN, firewall rules campione, connessioni cliente	Regole giustificate; accessi remoti tracciati; cambi di regole approvati.

10. Pacchetti evidenze per processo aziendale

Governo SGSI e Direzione

Campo	Contenuto
Owner / intervistati	CEO, GM, Qualita, Responsabile Sicurezza
Evidenze da raccogliere	Politica SGSI; Scopo; Risk assessment; SoA; Obiettivi; Riesame Direzione; Budget/risorse; Piano miglioramento
Criteri di accettazione	Evidenze firmate e datate; Input/output riesame completi; Azioni tracciate con owner e scadenza
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

Sviluppo software e release

Campo	Contenuto
Owner / intervistati	Area tecnica, F. Sergio, G. Casale, A. Rivoli, A. Minasi
Evidenze da raccogliere	SDLC; repository access; code review; test report; release notes; change approval; vulnerability remediation
Criteri di accettazione	Tracciabilita requisito-change-test-release; Separazione ambienti; Accessi repo coerenti con ruoli
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

Sistemistica, data center e sicurezza tecnica

Campo	Contenuto
Owner / intervistati	C. De Luca
Evidenze da raccogliere	Inventario; schema rete; MFA; access review; patching; backup; restore; monitoring; incident log
Criteri di accettazione	Asset critici sotto controllo; prove tecniche recenti; scostamenti gestiti con risk treatment
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

Help desk, assistenza e clienti

Campo	Contenuto
Owner / intervistati	F. Natale, C. Munno, A.S. Valente
Evidenze da raccogliere	ticket campione; procedure reset; accessi remoti; SLA; session log; autorizzazioni cliente; report intervento
Criteri di accettazione	Ogni intervento tracciato; identita/approvazione verificata; incidenti distinti da richieste ordinarie
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

Call/contact center

Campo	Contenuto
Owner / intervistati	D. Landolfi
Evidenze da raccogliere	script; training operatori; profili accesso; registrazioni/retention; audit postazioni; quality monitoring
Criteri di accettazione	Trattamento dati coerente con privacy e minimizzazione; operatori formati; accessi profilati
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

Commerciale, gare e contratti

Campo	Contenuto
Owner / intervistati	GM, M. Annunziata, C. Bernardino, I. Pasquariello
Evidenze da raccogliere	offerte; contratti; NDA; clausole sicurezza; requisiti cliente; supplier/customer docs
Criteri di accettazione	Requisiti sicurezza recepiti prima della firma; documenti riservati protetti; variazioni tracciate
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

HR, qualita e competenze

Campo	Contenuto
Owner / intervistati	L. Viggiano
Evidenze da raccogliere	mansionario; organigramma; matrice competenze; formazione; onboarding/offboarding; audit interni; NC/AC
Criteri di accettazione	Coerenza persone-ruoli-accessi; formazione completa; azioni chiuse o pianificate
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

R&S e progetti innovativi

Campo	Contenuto
Owner / intervistati	S. De Vita
Evidenze da raccogliere	registro progetti; NDA; accessi repository; dati test; valutazioni privacy/security; deliverable
Criteri di accettazione	Dati protetti e minimizzati; partner regolati; IP classificata e protetta
Campionamento consigliato	Selezionare almeno 3 campioni nel periodo: un caso ordinario, un caso critico e un caso con anomalia/variante/ritardo, collegandoli a rischio e controllo.

11. Piano interviste e campionamento per dipendente/funzione

Il piano interviste deve evitare risposte generiche. Ogni intervista deve essere collegata a una prova reale, preferibilmente estratta a video da sistemi attivi e poi salvata in audit room con data, owner e riferimento al controllo.

Intervistato/funzione	Focus audit	Campioni da chiedere	Esito atteso
CEO / Pasquale Russo	Leadership, risorse, rischio residuo, obiettivi, miglioramento	Riesame Direzione; approvazione risk treatment; KPI; risorse stanziate	Dimostra commitment e decisioni basate su dati SGSI.
GM / Mario Alessandro Russo	Requisiti cliente, contratti, SLA, comunicazione	2 contratti/offerte con requisiti security; comunicazione cliente; variazione contrattuale	Requisiti sicurezza tradotti in impegni e controlli.
Qualita/HR / L. Viggiano	Document control, competenze, audit, NC/AC, formazione	Registro documenti; training; audit interno; offboarding; azioni correttive	Sistema documentato, aggiornato e verificabile.
Sicurezza/Sistemistica / C. De Luca	Controlli tecnici, backup, patch, accessi, logging	Access review; backup restore; vuln scan; log VPN/MFA; incident register	Controlli tecnici vivi e coerenti con rischi.
Area tecnica / A. Minasi	Change, architetture, release e ambienti	Change critico; test; release; segregazione ambienti; diagramma architettura	Modifiche controllate e rischi tecnici valutati.
Team WH/cartella / F. Sergio	Secure development su applicazioni cliniche	Pull request/commit; bug fix; test sicurezza; release approvata	Codice e rilasci tracciati e verificati.
Team territorio / G. Casale	Telemedicina, integrazioni, accessi esterni	Log accessi; test API; ticket integrazione; monitoraggio uptime	Servizi territoriali protetti e tracciati.
Team APP / A. Rivoli	API, app, build/release, segreti	Pipeline release; dependency scan; API auth; secrets management	Sicurezza applicativa documentata.
Help desk / F. Natale	Reset, richieste accesso, ticket incidenti	Ticket reset; ticket accesso; escalation incidente; KB procedure	Identificazione utente e tracciabilita dimostrate.
Assistenza / C. Munno	Accessi remoti, interventi cliente, ticket	Session log; ticket assistenza; autorizzazione cliente; account nominativo	Accesso cliente autorizzato e documentato.
Call Center / D. Landolfi	Protezione dati in contatto telefonico	Script; formazione; profili; retention registrazioni; audit postazioni	Operatori istruiti e dati protetti.
R&S / S. De Vita	IP, dati di progetto, partner	NDA; accessi repository; registro dataset; deliverable; valutazione privacy	Know-how e dati progettuali protetti.
Commerciale/Gare / M. Annunziata, C. Bernardino, I. Pasquariello	Offerte, gare, requisiti, contratti	Offerta con security requirements; NDA; archivio gare; approvazioni	Riservatezza e requisiti contrattuali presidiati.

12. Struttura audit room consigliata

Per un livello enterprise, l audit room non deve essere una raccolta casuale di file. Deve avere naming convention, indice, owner, periodo, stato e collegamento a clausola ISO, controllo Annex A, rischio e asset.

Cartella	Contenuto	Owner	Nome file consigliato
00_Indice_Audit_Room	Indice master, elenco evidenze, tracker richieste auditor	Qualita	00_Index_AuditRoom_GESAN_ISO27001_YYYYMMDD.xlsx/pdf
01_Scope_Context_Leadership	Scopo, contesto, parti interessate, politica, obiettivi, organigramma, mansionario	Qualita / Direzione	01_Scope_Context_Roles_vYYYYMMDD.pdf
02_Risk_SoA_Treatment	Metodologia rischio, risk register, SoA, piano trattamento, accettazioni	Sicurezza / Qualita	02_RiskRegister_SoA_Treatment_vYYYYMMDD.xlsx/pdf
03_Asset_Register	Inventario asset, classificazione, owner, CIA, sedi, applicazioni	Sicurezza / owner asset	03_AssetRegister_GESAN_YYYYMMDD.xlsx
04_Access_Management	Policy accessi, richieste, revoche, review, admin, MFA, VPN	Sicurezza / Help Desk / HR	04_AccessReview_SemestreX_YYYY.pdf
05_Secure_Development_Change	SDLC, change, release, code review, test, vulnerabilita applicative	Area Tecnica / Team	05_Change_Release_Sample_ID.pdf
06_Infrastructure_Backup_Logging	Backup, restore, patching, hardening, log, monitoring, network	Sistemistica	06_RestoreTest_SystemName_YYYYMMDD.pdf
07_Incident_NC_AC	Incident register, NC/AC, RCA, lessons learned	Qualita / Sicurezza	07_IncidentRegister_Q1-Q4_YYYY.xlsx
08_Suppliers_Contracts	Fornitori, contratti, SLA, clausole, valutazioni, subfornitori	Amministrazione / GM / Sicurezza	08_VendorSecurityAssessment_YYYY.xlsx
09_HR_Training_Awareness	Formazione, competenze, onboarding/offboarding, prese visione	HR / Qualita	09_TrainingMatrix_ISMS_YYYY.xlsx
10_CallCenter_Support	Script call center, ticket help desk/assistenza, report SLA, accessi remoti	Call Center / Supporto	10_Support_CallCenter_EvidencePack_YYYY.pdf
11_InternalAudit_ManagementReview	Audit interno, piano audit, rapporti, riesame Direzione, KPI	Qualita / Direzione	11_InternalAudit_ManagementReview_YYYY.pdf

12.1 Naming convention enterprise

Tipo evidenza	Formato consigliato	Esempio
Registro	GESAN_ISMS_[Registro]_[Periodo]_[Version e]_[Data]	GESAN_ISMS_RiskRegister_2026_v1_20260505.xlsx
Campione tecnico	GESAN_ISMS_[Controllo]_[Sistema]_[IDticket]_[Data]	GESAN_ISMS_RestoreTest_DBClinico_TCK12345_20260418.pdf
Verbale	GESAN_ISMS_[Riunione]_[Data]_[Rev]	GESAN_ISMS_ManagementReview_20260430_Rev01.pdf
Evidenza accessi	GESAN_ISMS_AccessReview_[Ambito]_[Periodo]	GESAN_ISMS_AccessReview_Admin_Q2-2026.pdf

13. Valutazione maturita evidenze prima della sorveglianza

Prima dell audit assegnare a ogni pacchetto evidenza un punteggio da 1 a 5. L obiettivo minimo consigliato per una sorveglianza solida e 4/5 su aree critiche e 3/5 sulle aree non critiche, con piano azioni per ogni gap.

Livello	Significato	Indicatore pratico
1 - Assente	Documento o evidenza non disponibile	Il responsabile non sa mostrare registrazioni nel periodo.
2 - Formale	Documento esiste ma non e collegato a log, ticket, rischi o owner	Policy/procedura presente ma senza prove di esecuzione.
3 - Operativo	Evidenze presenti ma parziali o non sistematiche	Campioni disponibili, ma non sempre collegati a risk register/SoA.
4 - Gestito	Evidenze complete, tracciate, con KPI e review	Owner, scadenze, trend, azioni e controlli dimostrabili.
5 - Ottimizzato	Sistema predittivo e migliorativo	Automazione, dashboard, trend, lessons learned e miglioramento continuo dimostrati.

13.1 Gap critici da chiudere prima dell audit

Gap potenziale	Rischio audit	Azione correttiva preventiva
Organigramma e mansionario non allineati a ISO 27001	Osservazione o NC su ruoli/responsabilita	Emettere matrice RACI SGSI e nomine owner asset/rischi.
Responsabile Sicurezza nominato in organigramma ma senza mandato SGSI formalizzato	Debolezza nella accountability dei controlli tecnici	Nomina formale con perimetro: accessi, incidenti, backup, vulnerability, SoA tecnica.
Asset inventory non collegato a owner e CIA	Debolezza in risk assessment e SoA	Aggiornare inventario con asset owner, classificazione, criticita e ubicazione.
Access review incompleta	Possibile NC su privilegi e least privilege	Eseguire review utenti/privilegi per sistemi critici e repository.
Backup senza restore test recente	Rischio NC su disponibilita e continuita	Eseguire restore test documentato su almeno un sistema critico.
SDLC senza evidenze di security review	Rischio NC su sviluppo sicuro	Predisporre checklist OWASP, code review e campione release sicura.
Call center senza script privacy/security aggiornati	Rischio su divulgazione dati	Aggiornare script identificazione, training operatori e audit postazioni.

14. Piano operativo 30 giorni prima dello stage di vigilanza

Quando	Attivita	Owner	Output atteso
T-30 / T-25	Congelare perimetro, organigramma, mansionario, sedi, asset critici e owner; definire audit room index	Qualita / Direzione	Indice audit room; RACI; elenco owner
T-25 / T-20	Aggiornare risk assessment, SoA e piano trattamento; verificare rischi su data center, sviluppo, call center, assistenza	Sicurezza / Qualita	Risk register e SoA aggiornati
T-20 / T-15	Raccogliere evidenze tecniche: access review, backup/restore, vulnerability, patch, log, incidenti, change	C. De Luca / Area tecnica	Pacchetto tecnico completo
T-15 / T-12	Raccogliere evidenze sviluppo: repository, code review, test, release, change, gestione bug	A. Minasi / team applicativi	Pacchetto SDLC e release
T-12 / T-10	Raccogliere evidenze HR, formazione, awareness, onboarding/offboarding e prese visione	L. Viggiano	Matrice competenze e formazione
T-10 / T-8	Raccogliere evidenze help desk, assistenza, call center e customer care	F. Natale / C. Munno / D. Landolfi	Ticket, script, formazione, report SLA
T-8 / T-6	Verificare contratti, fornitori, offerte e clausole sicurezza/privacy	GM / Amministrazione / Commerciale	Vendor register, contratti campione, NDA
T-6 / T-4	Eseguire audit interno mirato su gap critici e chiudere evidenze mancanti	Qualita / Auditor interni	Report audit interno e NC/AC
T-4 / T-2	Riesame Direzione straordinario o integrazione riesame: rischi, KPI, incidenti, azioni, risorse	Direzione / Qualita	Verbale riesame aggiornato
T-1	Dry run con intervistati e verifica audit room	Qualita / Sicurezza	Check finale pronto audit

14.1 Checklist finale del consulente senior

Check	Domanda chiave	Esito atteso
Perimetro	Lo scopo riflette sedi, servizi, data center, sviluppo, supporto e call center?	Si, con coerenza tra visura, sito, organigramma e asset.
Responsabilita	Ogni processo ha un owner nominativo?	Si, con RACI e nomine/mandati.
Asset	Ogni asset critico ha owner e classificazione?	Si, con inventario aggiornato.
Rischi	Ogni rischio alto ha trattamento e stato?	Si, con piano azioni e accettazione residua.
Controlli	La SoA e allineata alle evidenze?	Si, nessun controllo dichiarato implementato senza prova.
Tecnico	Backup, accessi, patch, log e vulnerabilita sono dimostrabili?	Si, con report recenti e campioni.
Persone	Formazione e accessi sono coerenti con mansioni?	Si, con training, job description e access review.
Miglioramento	NC, incidenti e KPI generano azioni?	Si, con RCA e verifica efficacia.

15. Appendici integrate e indicazioni di validazione

Nelle pagine successive del PDF sono accodati come allegati tecnici i documenti di origine disponibili in formato PDF o convertiti: mansionario aziendale, organigramma funzionale e visura camerale. L inclusione degli allegati consente all auditor e alla Direzione di verificare immediatamente la base documentale utilizzata per la matrice V2.

Allegato	Documento	Uso in audit
A	Allegato 2 - Mansionario aziendale GESAN, convertito da DOC a PDF	Validare ruoli, responsabilita, mansioni, riferimenti a DGE/RD/RSGQ/AMM/COM/ACQ/SER/DT.
B	Allegato 3 - Organigramma funzionale GESAN	Validare nominativi, funzioni, linee di riporto e interlocutori audit.
C	Visura GESAN S.r.l.	Validare sedi, attivita esercitate, unita locali, addetti e oggetto operativo rilevante per lo scopo.

Punto di attenzione: il raccordo tra organigramma e mansionario deve essere formalizzato internamente. In particolare, per ruoli quali Responsabile Sicurezza, DGE/RD, RSGQ, owner applicativi, owner asset e risk owner, si raccomanda l emissione di nomine o di una matrice RACI approvata dalla Direzione.

INDICE

DIRETTORE GENERALE PER LA QUALITA' (DGE)

E' per definizione responsabile della società ed esprime direttamente gli indirizzi aziendali così come sono stati determinati nella Mission e nella Politica per la Qualità aziendale.

E' il primo responsabile della qualità ed in particolare ha il compito di:

- verificare l'idoneità dell'organizzazione aziendale e dell'adeguatezza delle risorse in ordine alla gestione per la qualità e la formulazione della Politica per la Qualità e degli obiettivi e dei budget aziendali;
- effettuare il riesame periodico del Sistema di gestione per la Qualità (vedi **punto Riesame da parte della Direzione** e procedura **Modalità di definizione delle Politiche e degli obiettivi aziendali e gestione dei riesami**);

E', inoltre, responsabile della:

- **Gestione delle risorse umane**:
  Da DGE dipendono le scelte in termini di esigenze; ha la responsabilità della scelta del personale, della pianificazione dei bisogni in termini di addestramento e formazione e del controllo e del monitoraggio del personale operatore attraverso registrazioni apposite (vedi **Gestione delle Risorse Umane**); gestisce i rapporti contrattuali con il personale aziendale e tutte le eventuali variazioni di organico nel rispetto delle indicazioni delle Leggi di riferimento cogenti.

- **Gestione e controllo del sistema qualità aziendale**:
  - approvare i documenti della Qualità e degli altri sistemi di gestione emessi;
  - programmare le attività di verifica ispettiva interna;
  - promuovere, nelle dovute forme e modalità, l'esecuzione di Azioni di miglioramento, Correttive o Preventive, e verificarne in seguito l'attuazione, l'esito e l'efficacia;
  - effettuare valutazioni in merito alla Soddisfazione Cliente;

- **Relazioni con l'esterno:**
  Gestisce le relazioni con l'esterno in termini di contatti con nuovi e/o potenziali clienti; si occupa dell'analisi e della ricerca di nuovi mercati, del potenziamento di quelli esistenti e dell'attività di promotion in genere allo scopo di realizzare una maggiore visibilità di DGE sul proprio mercato di riferimento. Gestisce altresì i rapporti con Istituzioni, enti, associazioni.

- **Gestione commerciale:**
  Interviene nella predisposizione dei preventivi in termini di definizione dei prezzi; più in generale è responsabile dei rapporti con i clienti nella gestione delle attività contrattuali; verifica e avvalla le offerte emesse dal responsabile commerciale.

- **Gestione acquisti:**
  interviene nelle scelte aziendali in merito alle necessità di approvvigionamento, sulla base delle indicazioni provenienti dal Servizio Commerciale, e quindi in coordinamento con il Responsabile Commerciale.

  interviene nelle scelte aziendali in merito alle necessità di approvvigionamento, sulla base delle indicazioni provenienti dal Servizio Commerciale, e quindi in coordinamento con il Responsabile Commerciale.

RAPPRESENTANTE DELLA DIREZIONE (RD)

E' designato dal vertice aziendale ed, indipendentemente da altre sue responsabilità, assume la responsabilità e l'autorità per:

1- Assicurare che i processi necessari per il sistema di gestione della qualità siano predisposti, attuati e tenuti aggiornati

2- riferire all'alta direzione sulle prestazioni del sistema di gestione per la qualità e su ogni esigenza per il miglioramento continuo

3- Assicurare la promozione della consapevolezza dei requisiti regolamentari e del cliente nell'ambito di tutta l'organizzazione

PERSONA RESPONSABILE DEL RISPETTO DELLA NORMATIVA REG (UE) 2017/745 (REG-UE)

La persona responsabile del rispetto della normativa ha il compito di assicurarsi che:

1- la conformità dei dispositivi sia adeguatamente controllata in conformità al sistema di gestione della qualità in base al quale i dispositivi vengono fabbricati, prima che un prodotto (dispositivo medico) venga rilasciato;

2- la documentazione tecnica e la dichiarazione di conformità siano redatte e aggiornate;

3- siano soddisfatti gli obblighi di sorveglianza post-commercializzazione secondo gli articoli di riferimento;

4- siano soddisfatti gli obblighi di segnalazione di incidenti;

5-siano soddisfatti gli obblighi di segnalazione di cui agli articoli da 82 a 86 del REG (UE) 2017/745;

6- nel caso di dispositivi destinati agli studi delle prestazioni da utilizzare nell'ambito di studi interventistici relativi alle prestazioni cliniche o altri studi delle prestazioni che comportano rischi per i soggetti degli studi, venga rilasciata la dichiarazione prevista.

RESPONSABILE QUALITA' (RSGQ)

Ha l'autorità e la responsabilità della gestione di tutti gli aspetti riferiti al sistema qualità aziendale e contenuti nel presente Manuale Qualità e nei documenti – procedure, istruzioni e moduli - ad esso afferenti, assicurandone la corretta e puntuale applicazione nel tempo.

RSGQ ha la responsabilità **in relazione agli aspetti di gestione del sistema per la qualità**, ed ha il compito di:

- preparare, revisionare e distribuire in maniera controllata il Manuale Qualità ed i documenti ad esso afferenti;
- avere cura, per quanto di sua competenza, dell'archiviazione dei documenti relativi al Sistema di gestione per la Qualità;
- verificare, se il caso, che i documenti emessi dalle funzioni interne o provenienti da enti esterni contengano le informazioni e le prescrizioni di qualità;
- eseguire e coordinare, secondo le modalità previste, periodiche Visite Ispettive Interne nelle diverse aree aziendali;
- promuovere, nelle dovute forme e modalità, l'esecuzione di Azioni di miglioramento, Correttive o Preventive, e verificarne in seguito l'attuazione, l'esito e l'efficacia;
- verificare, unitamente ai responsabili preposti, la validità di tutte le norme utilizzate dalle varie funzioni aziendali;
- predisporre ed ordinare, nelle dovute forme, i documenti da sottoporre al DGE per il Riesame della Direzione;
- gestire il piano di controllo qualità, le modalità di controllo di qualità sia all'interno dell'organizzazione che per i processi in outsourcing;
- gestire i rapporti con i Clienti, con i fornitori e con gli Organismi di Certificazione, per tutti gli aspetti relativi alla Garanzia Qualità;
    - si occupa dell'invio a Cliente e della successiva raccolta dei Questionari di Soddisfazione Cliente;

Riferisce direttamente alla DGE.

RESPONSABILE SERVIZIO PREVENZIONE E PROTEZIONE (RSPP)

Ha la responsabilità delle azioni da intraprendere per l'adeguamento al d.Lgs. 81/2008 e S.m.i. in materia di sicurezza sul lavoro**.**
Relativamente ai sistemi di gestione del servizio prevenzione e protezione, RSPP ha la responsabilità di gestire e coordinare tali attività nel rispetto delle disposizioni di Legge vigenti.
L'RSPP gestisce il servizio di prevenzione e protezione che provvede:
a) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la
sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica
conoscenza dell'organizzazione aziendale;
b) ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28 comma 2 d.Lgs. 81/2008 e S.m.i., e i sistemi di controllo di tali misure;
c) ad elaborare le procedure di sicurezza per le varie attività aziendali;
d) a proporre i programmi di informazione e formazione dei lavoratori;
e) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35 d.Lgs. 81/2008 e S.m.i.;
f) a fornire ai lavoratori le informazioni di cui all'articolo 36 d.Lgs. 81/2008 e S.m.i..

RESPONSABILE PRODUZIONE (PROD)

Il responsabile di produzione risponde al Direttore generale (DGE).
E' responsabile della gestione delle risorse di personale e delle attrezzature del reparto produttivo, in conformità alla pianificazione aziendale approvata dal Direttore Generale.

Principali attività

- Attua le strategie aziendali relative alla produzione
- Assicura operativamente la disponibilità delle risorse e delle informazioni necessarie per supportare il funzionamento e il monitoraggio dei processi aziendali, tenendo conto, con il contributo degli indicatori, dell'andamento generale dell'azienda e dei risultati economici.
- Assicura il supporto tecnico necessario al personale così da poter eseguire il lavoro in modo preciso e pulito.
- Sorveglia costantemente la produttività, contenendo al massimo i tempi morti o improduttivi.
- Motiva e istruisce il personale operativo nell' ambito delle proprie mansioni.
- Raccoglie e analizza i dati dei processi a lui assegnati.
- Controlla le campionature dei fornitori.
- Blocca qualsiasi attività sui prodotti quando non corrisponde alle esigenze.
- Stabilisce i metodi di controllo della qualità.
- Conduce e istruisce dal lato tecnico i responsabili ai controlli.
- Collabora con l'ufficio tecnico allo sviluppo dei nuovi prodotti.
- Gestisce e sorveglia gli strumenti di misura.
- Gestisce gli strumenti e i mezzi di produzione e sorveglia la manutenzione.
- Informa la vendita su eventuali ritardi nell'evasione degli ordini.
- Organizza le riunioni di produzione.
- Applica nel proprio ambito quanto definito nelle procedure operative.
- Gestire le schede di sicurezza dei prodotti pericolosi.

A lui si rivolgono gli altri uffici per informazioni relative alla produzione.

RESPONSABILE MAGAZZINO (MAG)

Il responsabile di magazzino è responsabile della movimentazione e dello stoccaggio dei materiali. Ha il compito di gestire le aree del magazzino, in termini di identificazione e di separazione e di assicurare che le condizioni rimangano inalterate.

RESPONSABILE SERVIZIO AMMINISTRAZIONE (AMM)

La Funzione amministrazione ha il compito di amministrare le vendite (gestione vendite, fatture, compilazione scadenziari) e gli acquisti (ricevimento bolle e fatture, compilazione scadenziari).
La Funzione amministrazione ha il compito di gestire i dati contabili, di garantirne esattezza e veridicità, e di assicurare la corretta gestione contabile ed amministrativa dell'azienda.
Riceve dal consulente del lavoro le buste paga che distribuisce ai dipendenti.
Propone ed attua indirizzi ed azioni per il costante miglioramento delle attività di competenza.
AMM inoltre coadiuva DGE e PROD nella gestione delle attività relative all'addestramento del personale, curandone la registrazione in apposita modulistica.
Collabora con DGE nella registrazione delle attività di manutenzioni sui mezzi e sulle attrezzature.
Periodicamente ha il compito di analizzare e sottoporre all'attenzione della Direzione i dati necessari ad effettuare analisi statistiche relativamente ai dati finanziari.

RESPONSABILE SERVIZIO COMMERCIALE (COM)

Il responsabile commerciale si occupa della gestione documentale delle trattative commerciali con i Clienti, dall'acquisizione delle richieste Clienti all'emissione, alla conservazione e all'archiviazione della documentazione che si genera in queste fasi:

- raccoglie le richieste dei Clienti;
- in collaborazione con DGE e ACQ effettua le indagini fornitori per la predisposizione dei preventivi cliente / listini prezzi;
- predispone il documento di offerta/preventivo e ne tiene registrazione;
- conserva tutta la documentazione che si genera nella predisposizione delle offerte/preventivi e più in generale di natura contrattuale in appositi raccoglitori;
- gestisce eventuali problemi e le modifiche contrattuali VARIANTI, coordinando in questo senso il DGE;
- ha il compito di registrare eventuali Non conformità rilevate.

Attua le politiche di post vendita curandone la pianificazione di dettaglio.

RESPONSABILE SERVIZIO ACQUISTI (ACQ)

Il Responsabile Acquisti ha la responsabilità di:

- valutare, selezionare e monitorare nel tempo i fornitori di materiali, attrezzature e di servizi professionali aventi diretta influenza sulla qualità dei servizi di attestazione forniti;
- richiedere preventivi, predisporre, verificare, firmare ed emettere, nel rispetto delle normative di riferimento vigenti, gli ordini di approvvigionamento e gli eventuali contratti con i fornitori;
- registrare eventuali Non conformità rilevate sul Rapporto di Non Conformità e successivamente di consegnarlo a RSGQ;

Il Responsabile Acquisti collabora con il servizio commerciale per la predisposizione dei preventivi Clienti / listini prezzi.

RESPONSABILE DEI SERVIZI DI INSTALLAZIONE E MANUTENZIONE (SER)

Il Responsabile SER si occupa prevalentemente della gestione dell'installazione dei macchinari prodotti dall'azienda presso i clienti della stessa. Provvede, inoltre, ad eseguire la manutenzione degli stessi presso le imprese clienti.

I compiti principali del responsabile di gestione e manutenzione sono:

- assicurare la corretta manutenzione dei prodotti;
– assicurare il corretto utilizzo delle risorse interne;
– organizzazione, coordinamento e controllo dell'attività del personale specialistico;
– interventi di ripristino e manutenzione;
– garanzia del rispetto delle normative di sicurezza e l'applicazione delle norme di buona fabbricazione;
– garanzia della buona esecuzione dei lavori nel rispetto dei costi standard previsti.

DIRETTORE TECNICO (DT)

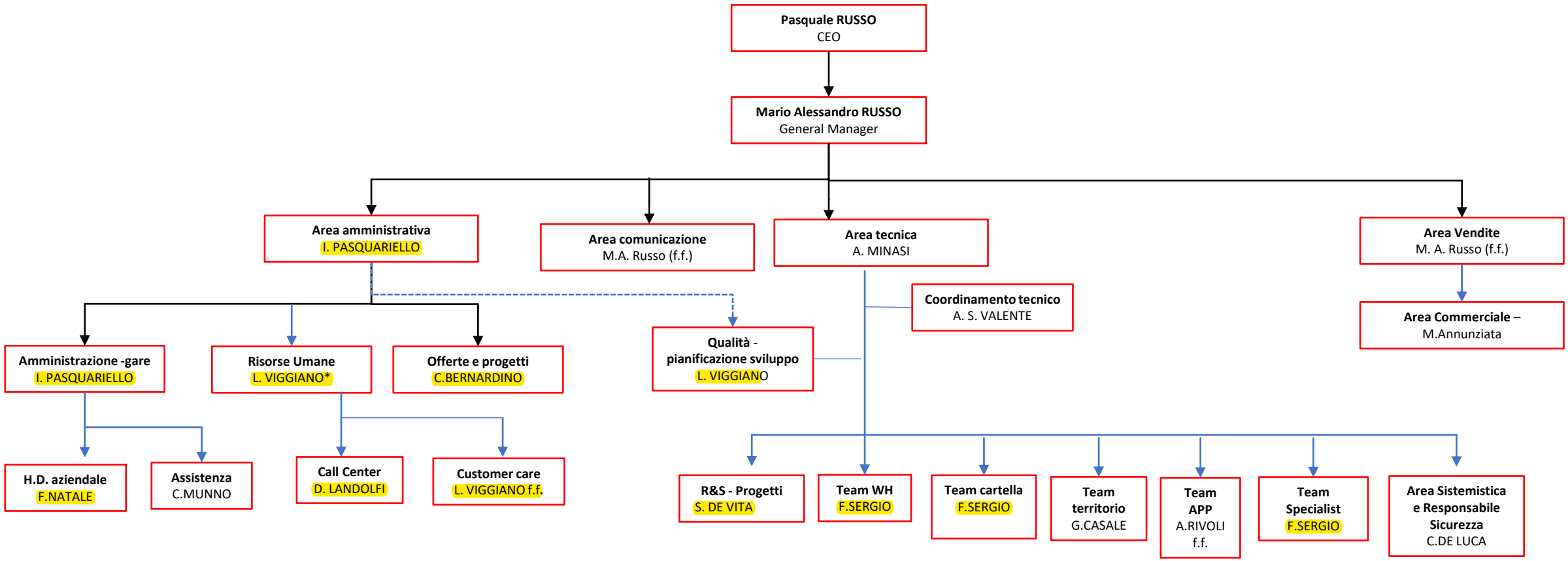
Il DT contribuisce alla direzione della Società, collaborando al suo sviluppo tecnologico, assiste la Direzione Generale nella definizione e nella direzione del sistema di governo, rappresentando un supporto per la formulazione e l'applicazione delle politiche e per la pianificazione strategica. E', inoltre, garante della correttezza, completezza e trasparenza dei processi di formazione dei documenti rappresentativi delle dinamiche tecniche e tecnologiche della Società.

I compiti principali del DT sono:

- sovrintendere alla gestione del Dipartimento Ufficio Tecnico;
- sovrintendere ai rapporti con i fruitori ed i clienti dei servizi erogati dalla Società, per quanto riguarda l'aspetto tecnico
- sovrintendere alla gestione delle commesse e assicurare il rispetto delle scadenze per il loro avanzamento dal punto di vista tecnico
- sovrintendere all'elaborazione dei disegni tecnici e degli ordini clienti e fornitori
- studiare e identificare le soluzioni tecniche per aumentare la sinergia tra i vari progetti aziendali
- collaborare alla programmazione della produzione e delle offerte economiche
- conoscere gli obiettivi e le politiche aziendali e di gruppo
- collaborare con la Direzione Generale alla definizione di nuovi obiettivi generali della gestione aziendale
- proporre alla Direzione Generale iniziative volte alla razionalizzazione dei servizi tecnici e allo snellimento delle procedure
- essere di supporto all'Ente Commerciale nel verificare la fattibilità dei progetti - assistere la Direzione Generale nelle relazioni periodiche sull'andamento della filiale, fornendo opportune analisi
- mantenere il costante aggiornamento su tutta la materia di competenza
- divulgare al proprio settore ed agli altri settori aziendali gli aggiornamenti normativi di propria competenza che hanno riflessi sulle loro attività
- assicurare la tenuta e l'aggiornamento degli archivi e dei back-up informativi pertinenti al settore di responsabilità
- assicurare la puntuale e corretta elaborazione dei report, accompagnandoli con relazioni di analisi di scostamento
- mantenere e migliorare la motivazione e la professionalità dei collaboratori assegnando loro obiettivi e compiti, promuovendo la competenza professionale e valutandone i risultati. Curare, attraverso la Predisposizione di specifici piani, l'aggiornamento e lo sviluppo delle risorse assegnate
- verificare l'osservanza dei doveri d'ufficio da parte del personale dell'Ufficio Tecnico
- applicare e far rispettare le direttive, le politiche e le procedure aziendali e di gruppo dai collaboratori
- controllare, al fine di verificare la congruità economica, l'affidamento di consulenze, collaborazioni ed incarichi professionali

- relazionare periodicamente il diretto superiore sull'andamento del settore di responsabilità. Concordare ed applicare miglioramenti e rettifiche alle linee di condotta.
- assicurare la direzione e il controllo delle attività tecniche e di gestione commesse sviluppate dai capi commessa

ORGANIGRAMMA FUNZIONALE



*Il responsabile della Qualità ricopre anche il ruolo di DGE

CAMERA DI COMMERCIO CASERTA

Camera di Commercio Industria Artigianato e Agricoltura di CASERTA

Registro Imprese - Archivio ufficiale della CCIAA

VISURA ORDINARIA DI UNITA' LOCALE O SEDE SECONDARIA

GESAN S.R.L.

ETPEHT

Il QR Code consente di verificare la corrispondenza tra questo documento e quello archiviato al momento dell'estrazione. Per la verifica utilizzare l'App RI QR Code o visitare il sito ufficiale del Registro Imprese.

DATI ANAGRAFICI

Indirizzo Sede legale	(NA)
Numero REA	CE - 166528
Codice fiscale e n.iscr. al Registro Imprese	06693080639
Forma giuridica	societa' a responsabilita' limitata

Indice

1 Informazioni della posizione in provincia

Indirizzo Sede legale	(NA)
E-mail	gesan@gesan.it
Numero repertorio economico amministrativo (REA)	CE - 166528

2 Informazioni dell'Impresa

Registro Imprese	Codice fiscale e numero di iscrizione: 06693080639 Sezioni: Iscritta nella sezione ORDINARIA

iscrizione Registro Imprese	Codice fiscale e numero d'iscrizione: 06693080639 del Registro delle Imprese di NAPOLI
estremi della sede	Numero repertorio economico amministrativo: NA - 1106954
sezioni	Iscritta nella sezione ORDINARIA
partita iva	02364520615

3 Scioglimento e liquidazione, cancellazione

Cancellazione, cessazione e trasferimento

trasferimento	trasferimento in altra provincia in data 07/03/2024

4 Attività, albi ruoli e licenze

Attività

Addetti
(elaborazione da fonte INPS)

Numero addetti della posizione rilevati nell'anno 2025
(Dati rilevati al 31/12/2025)

Addetti nel comune di SAN NICOLA LA STRADA (CE)
Unità locali: 7

	I trimestre	II trimestre	III trimestre	IV trimestre	Valore medio
Dipendenti	66	68	67	66	67
Indipendenti	0	0	0	0	0
Totale	66	68	67	66	67

5 Sedi secondarie ed unita' locali

Unita' Locale n. CE/7 VIA TORINO 14 SAN NICOLA LA STRADA (CE) CAP 81020
Unita' Locale n. CE/8 VIA ANTONIO PACINOTTI SNC SAN NICOLA LA STRADA (CE) CAP 81020

Unita' Locale n. CE/7

Sede Operativa
Data apertura: 16/01/2024

Indirizzo

SAN NICOLA LA STRADA (CE)
VIA TORINO 14 CAP 81020

Attivita' esercitata

IL 24/01/1997 ATTIVITA ESERCITATA DALL'IMPRESA :SERVIZI DI TELEMATICA,ROBOTICA,EIDOMATICA
IL 05/12/2003 E' INIZIATA L' ATTIVITA' DI RICERCA NELL'AMBITO DELL'ORGANIZZAZIONE SANITARIA
18/04/2006 CONSULENZA PER INSTALLAZIONE DI SISTEMI INFORMATICI E HARDWARE
EDIZIONI SOFTWARE
ALTRE REALIZZAZIONI DI SOFTWARE E CONSULENZA INFORMATICA
ELABORAZIONE ELETTRONICA DEI DATI
BANCHE DI DATI
MANUTENZIONE E RIPARAZIONE DI MACCHINE PER UFFICIO,APPARECCHIATURE E MATERIALE INFORMATICO.
ATTIVITA DEI CALL CENTER

Classificazione ATECO 2025 dell'attività

Codice: 62.90.09 - altre attività dei servizi connessi alle tecnologie dell'informazione e dell'informatica n.c.a.
Importanza: primaria Registro Imprese

Codice: 33.12.51 - riparazione e manutenzione di macchine e attrezzature per ufficio
Importanza: secondaria Registro Imprese

Codice: 58.29.00 - edizione di altri software
Importanza: secondaria Registro Imprese

Codice: 62.20.10 - attività di consulenza informatica
Importanza: secondaria Registro Imprese

Codice: 63.10.10 - fornitura di infrastrutture informatiche, hosting e attività connesse
Importanza: secondaria Registro Imprese

Codice: 63.10.2 - elaborazione dati
Importanza: secondaria Registro Imprese

Codice: 72.10 - ricerca e sviluppo sperimentale nel campo delle scienze naturali e dell'ingegneria
Importanza: secondaria Registro Imprese

Codice: 82.20.00 - attività dei call center
Importanza: secondaria Registro Imprese

Codice: 95.10.10 - riparazione e manutenzione di computer e periferiche
Importanza: secondaria Registro Imprese

Classificazione ATECORI 2007-2022 dell'attività

Codice: 62.09.09 - altre attivita' dei servizi connessi alle tecnologie dell'informatica nca
Importanza: primaria Registro Imprese

Codice: 33.12.51 - riparazione e manutenzione di macchine ed attrezzature per ufficio (esclusi computer, periferiche, fax)
Importanza: secondaria Registro Imprese

Codice: 58.29 - edizione di altri software a pacchetto (esclusi giochi per computer)
Importanza: secondaria Registro Imprese

Codice: 62.02 - consulenza nel settore delle tecnologie dell'informatica
Importanza: secondaria Registro Imprese

Codice: 63.11.1 - elaborazione dati
Importanza: secondaria Registro Imprese

Codice: 63.11.2 - gestione database (attivita' delle banche dati)
Importanza: secondaria Registro Imprese

Codice: 72.1 - ricerca e sviluppo sperimentale nel campo delle scienze naturali e dell'ingegneria
Importanza: secondaria Registro Imprese

Codice: 82.2 - attivita' dei call center
Importanza: secondaria Registro Imprese

Codice: 95.11 - riparazione e manutenzione di computer e periferiche
Importanza: secondaria Registro Imprese

Unita' Locale n. CE/8

Ufficio
Data apertura: 10/04/2026

Indirizzo

SAN NICOLA LA STRADA (CE)
VIA ANTONIO PACINOTTI SNC CAP 81020

Attivita' esercitata

SERVIZI DI INSTALLAZIONE SOFTWARE

6 Aggiornamento impresa

Data ultimo protocollo	10/04/2026