Evidenze oggettive Stage 2

ISO/IEC 27001 - Farmacie Italiane S.r.l. - Settore IAF 33

Documento di supporto alla compilazione del rapporto di audit Stage 2. Le evidenze sono formulate per l'inserimento nella sezione dedicata alle evidenze oggettive e alla verifica della conformita del SGSI.

AREA / CLAUSOLA	EVIDENZE OGGETTIVE STAGE 2	ESITO / NOTE AUDITOR
4.1 - Contesto dell'organizzazione	Analisi del contesto interno ed esterno; identificazione fattori organizzativi, tecnologici, normativi e di mercato; collegamento con servizi ICT, sistemi informativi, fornitori critici e perimetro IAF 33.	Evidenze coerenti con il campo di applicazione del SGSI. Requisito conforme.
4.2 - Parti interessate	Mappa delle parti interessate; requisiti di Direzione, personale, fornitori ICT, clienti, farmacie/parafarmacie, societa partecipate/controllate, autorita e soggetti regolatori; collegamento con requisiti GDPR, NIS2 e contrattuali.	Parti interessate e requisiti pertinenti identificati e presi in carico. Requisito conforme.
4.3 - Campo di applicazione	Documento di campo di applicazione SGSI; indicazione sedi, processi, sistemi informativi, servizi cloud, reti, asset informativi, fornitori critici e interfacce operative incluse nel perimetro.	Ambito definito, documentato e coerente con attivita e rischi. Requisito conforme.
4.4 - Processi SGSI	Mappa processi SGSI; descrizione interazioni tra governance, risk management, trattamento rischi, controlli Annex A, audit interno, riesame Direzione e miglioramento continuo.	Processi identificati e integrati secondo logica PDCA. Requisito conforme.
5.1 - Leadership	Verbali di riunione; riesame Direzione; approvazione politica, obiettivi, risk assessment, piano trattamento e SOA; interviste alla Direzione e ai referenti SGSI.	Evidente coinvolgimento della Direzione nel mantenimento del SGSI. Requisito conforme.
5.2 - Politica sicurezza informazioni	Politica per la Sicurezza delle Informazioni approvata; evidenza di comunicazione interna; presa visione da parte del personale; coerenza con obiettivi e campo di applicazione.	Politica definita, comunicata e coerente con il SGSI. Requisito conforme.
5.3 - Ruoli e responsabilita	Organigramma/funzionigramma SGSI; matrice ruoli e responsabilita; nomine o incarichi; responsabilita per risk assessment, accessi, fornitori, incidenti, continuita operativa e documentazione.	Ruoli assegnati, compresi e applicati nei processi. Requisito conforme.
6.1.1 - Rischi e opportunita	Registro rischi e opportunita; collegamento con contesto, parti interessate e requisiti cogenti; pianificazione azioni di trattamento e miglioramento.	Rischi e opportunita determinati e gestiti. Requisito conforme.
6.1.2 - Valutazione rischi	Metodologia di risk assessment; criteri di probabilita, impatto e accettabilita; registro rischi aggiornato; evidenze di rivalutazione in caso di cambiamenti.	Processo applicato in modo coerente e aggiornato. Requisito conforme.
6.1.3 - Trattamento rischi / SOA	Piano di trattamento rischi; SOA aggiornata; rischi residui approvati; collegamento tra rischi, controlli Annex A, azioni, responsabili e stato di attuazione.	Trattamento rischi documentato, approvato e tracciabile. Requisito conforme.
6.2 - Obiettivi sicurezza informazioni	Obiettivi SGSI aggiornati; indicatori/KPI; responsabili; target; frequenza di monitoraggio; stato avanzamento; collegamento con rischi e politica.	Obiettivi misurabili, monitorati e coerenti con il SGSI. Requisito conforme.
6.3 - Pianificazione modifiche	Registro modifiche SGSI/ICT; valutazione impatti e rischi; approvazioni; aggiornamento documentazione; verifica post-implementazione.	Modifiche pianificate, autorizzate e controllate. Requisito conforme.
7.1 - Risorse	Evidenze di risorse umane, tecniche e infrastrutturali disponibili; strumenti ICT; supporto fornitori; risorse per formazione, monitoraggio, backup e sicurezza.	Risorse adeguate alla complessita del perimetro IAF 33. Requisito conforme.
7.2 - Competenza	Matrice competenze; piano formazione; registri formazione; attestati; CV/esperienze dei referenti; verifica aggiornamento competenze SGSI e ICT.	Competenze definite, documentate e coerenti con i ruoli. Requisito conforme.
7.3 - Consapevolezza	Materiali di awareness; comunicazioni interne; evidenze di presa visione policy; formazione su phishing, credenziali, incidenti, protezione dati e uso corretto strumenti aziendali.	Personale consapevole di policy, responsabilita e impatti. Requisito conforme.
7.4 - Comunicazione	Piano comunicazione interna/esterna; canali di segnalazione eventi; comunicazioni a personale, Direzione, fornitori e parti interessate; modalita di escalation incidenti.	Comunicazioni definite, formalizzate e accessibili. Requisito conforme.
7.5 - Informazioni documentate	Elenco documenti SGSI; controllo revisioni; approvazioni; gestione accessi ai documenti; conservazione registrazioni; backup documentale; protezione da modifiche non autorizzate.	Documentazione controllata, aggiornata e protetta. Requisito conforme.

AREA / CLAUSOLA	EVIDENZE OGGETTIVE STAGE 2	ESITO / NOTE AUDITOR
8.1 - Controllo operativo	Procedure operative; asset inventory; gestione accessi; gestione backup; gestione incidenti; gestione fornitori; controllo modifiche; registrazioni operative.	Processi operativi pianificati e controllati. Requisito conforme.
8.2 - Rivalutazione rischi	Risk assessment aggiornato; evidenze di riesame per modifiche tecnologiche, fornitori, servizi cloud, infrastrutture e processi ICT; aggiornamento rischi residui.	Rivalutazioni effettuate e documentate. Requisito conforme.
8.3 - Attuazione trattamento rischi	Stato avanzamento piano trattamento; evidenze implementazione controlli; assegnazione responsabilita; monitoraggio azioni; verifica efficacia dei controlli.	Azioni attuate, tracciate e coerenti con la SOA. Requisito conforme.
9.1 - Monitoraggio e misurazione	KPI SGSI; report monitoraggio; stato obiettivi; andamento incidenti; stato backup; avanzamento trattamento rischi; verifica efficacia controlli.	Prestazioni SGSI monitorate con evidenze idonee. Requisito conforme.
9.2 - Audit interno	Programma audit interno; piano audit; rapporto audit interno del 08/06/2026; rilievi; azioni correttive; verifica copertura requisiti ISO/IEC 27001.	Audit interno pianificato, svolto e documentato. Requisito conforme.
9.3 - Riesame Direzione	Verbale riesame Direzione del 06/04/2026; input/output del riesame; decisioni; risorse; stato rischi; obiettivi; azioni di miglioramento.	Riesame svolto e coerente con requisiti ISO/IEC 27001. Requisito conforme.
10.1 - Miglioramento continuo	Registro miglioramenti; output audit interno; output riesame Direzione; aggiornamento obiettivi; azioni di rafforzamento controlli e consapevolezza.	Miglioramento continuo attivo e documentato. Requisito conforme.
10.2 - Non conformita e azioni correttive	Registro NC/azioni correttive; analisi cause; responsabilita; scadenze; stato azioni; verifica efficacia; chiusura rilievi Stage 1.	Processo efficace, tracciato e senza NC ostative. Requisito conforme.
Annex A - Governance e organizzazione	SOA; policy di sicurezza; ruoli e responsabilita; gestione fornitori; gestione asset; requisiti normativi; sicurezza nei progetti e nei processi ICT.	Controlli organizzativi applicati e coerenti con i rischi.
Annex A - Controlli persone	Piano formazione; awareness; responsabilita del personale; gestione accessi in ingresso/uscita; regole di comportamento e utilizzo sistemi.	Controlli sulle persone adeguati al perimetro SGSI.
Annex A - Controlli fisici	Misure di accesso fisico alle sedi; protezione postazioni; gestione aree operative; protezione apparati, rack, server e dispositivi ICT.	Controlli fisici proporzionati al contesto operativo.
Annex A - Controlli tecnologici	Gestione accessi; MFA; endpoint protection/EDR; backup; logging; sicurezza rete; VPN; protezione cloud; vulnerability assessment; controlli crittografici.	Controlli tecnologici implementati e verificati con esito positivo.
Vulnerability assessment / penetration testing	Report test; ambito verificato; classificazione vulnerabilita; piano remediation; evidenza assenza vulnerabilita critiche aperte ostative alla certificazione.	Processo di gestione vulnerabilita adeguato e integrato nel SGSI.
Controlli crittografici	Evidenze di crittografia su comunicazioni, servizi cloud, accessi remoti, backup e credenziali; gestione chiavi tramite controlli di accesso e responsabilita definite.	Crittografia applicata ove pertinente e coerente con la valutazione dei rischi.
Gestione fornitori ICT	Elenco fornitori critici; valutazioni fornitori; accordi/contratti; clausole di sicurezza; accessi remoti; monitoraggio prestazioni e sicurezza.	Supply chain ICT presidiata e coerente con Annex A.
Incident management	Procedura gestione incidenti; canali segnalazione; registro eventi/incidenti; escalation; responsabilita; collegamento con NIS2 e miglioramento.	Processo definito e operativo. Nessun incidente critico aperto.
Continuita operativa e backup	Piano continuita/DR; procedure backup; evidenze esecuzione backup; test o verifiche di ripristino; responsabilita operative.	Continuita e backup gestiti in modo coerente con il rischio.
Gestione reclami	Dichiarazione assenza reclami; eventuale registro reclami; processo di gestione collegato a segnalazioni, NC e azioni correttive.	Nessun reclamo aperto o ostativo alla certificazione.