

SGSI - Manuale

Agenzia delle entrate-Riscossione

Sommario

REVISIONI DEL DOCUMENTO	4
INTRODUZIONE	4
AGENZIA DELLE ENTRATE-RISCOSSIONE.....	4
IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	5
L'APPROCCIO PER PROCESSI.....	7
SEZIONE 1 – SCOPO E CAMPO DI APPLICAZIONE	8
SEZIONE 2 - RIFERIMENTI NORMATIVI	8
2.1 NORMATIVA E DOCUMENTI DI RIFERIMENTO	8
2.2 CORRELAZIONE TRA MANUALE E REQUISITI DELLA NORMA	10
SEZIONE 3 - TERMINI E DEFINIZIONI	10
3.1 SIGLE E ABBREVIAZIONI	10
3.2 TERMINI E DEFINIZIONI.....	11
SEZIONE 4 -CONTESTO DELL'ORGANIZZAZIONE	13
4.1 COMPRENDERE L'ORGANIZZAZIONE ED IL SUO CONTESTO	13
4.2 ESIGENZE ED ASPETTATIVE DELLE PARTI INTERESSATE	13
4.3 DOCUMENTI DEL SGSI	18
SEZIONE 5- LA LEADERSHIP.....	18
5.1 LEADERSHIP E IMPEGNO	18
5.2 POLITICA	19
5.3 RUOLI, RESPONSABILITÀ E AUTORITÀ NELL'ORGANIZZAZIONE.....	19
SEZIONE 6 – PIANIFICAZIONE	22
6.1 AZIONI PER AFFRONTARE RISCHI E OPPORTUNITÀ.....	22
6.2 OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI	23
SEZIONE 7 – SUPPORTO	24
7.1 RISORSE	24
7.2 COMPETENZA	24
7.3 CONSAPEVOLEZZA.....	24
7.4 COMUNICAZIONE	24
7.5 INFORMAZIONI DOCUMENTATE.....	24
SEZIONE 8 – ATTIVITÀ OPERATIVE.....	27
8.1 PIANIFICAZIONE E CONTROLLI OPERATIVI	27

8.2	VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI.....	28
8.3	TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI....	28
SEZIONE 9 – VALUTAZIONE DELLE PRESTAZIONI		28
9.1	MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE	28
9.1.1	DEFINIZIONI.....	30
9.2	AUDIT DI PRIMO LIVELLO	30
9.3	RIESAME DI DIREZIONE.....	31
SEZIONE 10 – MIGLIORAMENTO		32
10.1	NON CONFORMITÀ E AZIONI CORRETTIVE.....	33
10.2	MIGLIORAMENTO CONTINUO.....	33
ALLEGATO 1 - MATRICE DI CORRELAZIONE TRA IL MANUALE SGSI DI AGENZIA DELLE ENTRATE-RISCOSSIONE E LA NORMA ISO 27001.....		34

REVISIONI DEL DOCUMENTO

Titolo	SGSI - Manuale	Data	18/01/2021
Autore	Gestore SGSI	Riferimento	DIS_SGSI_Manuale SGSI_v2.0
Approvato da	Responsabile SGSI	Verificato da	Responsabile SGSI

INTRODUZIONE

AGENZIA DELLE ENTRATE-RISCOSSIONE

Agenzia delle entrate-Riscossione (di seguito Ente o AdeR) è un Ente Pubblico Economico istituito ai sensi dell'art. 1 del Decreto Legge n. 193/2016, convertito con modificazioni dalla Legge n. 225/2016, e svolge le funzioni relative alla riscossione nazionale. L'Ente è sottoposto all'indirizzo e alla vigilanza del Ministro dell'Economia e delle Finanze ed è strumentale all'Agenzia delle entrate a cui è attribuita la titolarità della riscossione nazionale ai sensi dell'art. 3, comma 1, del Decreto Legge n. 203/2005, convertito con modificazioni dalla Legge n. 248/2005. Agenzia delle entrate-Riscossione è subentrata, a titolo universale, nei rapporti giuridici attivi e passivi, anche processuali, delle società del gruppo Equitalia, sciolte a decorrere dal 1° luglio 2017 (a eccezione di Equitalia Giustizia). Il nuovo Ente Pubblico Economico ha autonomia organizzativa, patrimoniale, contabile e di gestione. La documentazione relativa all'organizzazione di AdeR è disponibile, e sempre aggiornata, in apposite sezioni della intranet dell'Ente.

Le attività istituzionali dell'Ente, connesse alla riscossione ed in generale tutte le altre attività previste dal funzionigramma, svolte dalle strutture dell'Ente, sono incentrate sulla gestione ed il trattamento di informazioni. A tal riguardo, riveste fondamentale importanza la protezione dei requisiti di riservatezza, integrità e disponibilità¹ delle informazioni. Il rispetto dei requisiti di sicurezza indicati, consente all'Ente di svolgere le proprie attività in modo corretto, con accuratezza, riducendo la possibilità di errori ed evitando conseguenze dannose in termini economici, di immagine e reputazionali.

L'Ente per poter garantire la sicurezza delle informazioni ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) che rappresenta l'insieme di politiche, processi, procedure, regole e ruoli, aventi lo scopo di controllare in modo sistematico e continuativo tutti gli aspetti inerenti alla sicurezza del patrimonio informativo. L'implementazione del sistema è stata avviata, a partire dal 2017, anche in considerazione di quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, emanato dall'Agenzia per l'Italia Digitale (AgID) che, tra le attività indicate alle singole amministrazioni per realizzare, strutturare, attuare e implementare i propri piani di

¹ La riservatezza garantisce che un'informazione sia accessibile solo a chi è autorizzato, l'integrità, salvaguarda l'accuratezza, l'autenticità e la completezza delle informazioni durante la loro creazione, elaborazione, trasmissione e ricezione, la disponibilità garantisce, quando richiesto e autorizzato, l'accesso alle informazioni e ai servizi associati.

sicurezza informatica, stabiliva che: “la Pubblica Amministrazione dovrà dotarsi di un Sistema di gestione della sicurezza delle informazioni (SGSI) e della relativa struttura organizzativa”.

Nella realizzazione del proprio SGSI, l'Ente ha deciso di avviare un percorso di implementazione in linea con quanto previsto dalla norma internazionale UNI EN CEI ISO IEC 27001:2017 (per brevità ISO 27001)² in materia di sicurezza delle informazioni. La norma definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni e considera non solo la sicurezza logica e tecnologica, ma include anche aspetti relativi alla sicurezza fisica ed organizzativa in quanto le informazioni sono gestite anche su documenti cartacei, sono conservate negli archivi e sono trattate dalle persone per lo svolgimento delle proprie mansioni.

La conformità del sistema alla norma, dimostrabile tramite un processo di certificazione gestito da un ente certificatore riconosciuto da Accredia³, garantisce ad AdeR di provare alle Parti Interessate (es. Agenzia delle entrate, i dipendenti, i contribuenti) di proteggere adeguatamente le informazioni. **A fine 2019, la conformità del SGSI dell'Ente alla norma ISO 27001 è stata dimostrata grazie all'ottenimento della certificazione ISO 27001 del SGSI per il primo perimetro di analisi relativo ai “Servizi IT e processi di gestione del Data Center”.**

Il presente documento ha l'obiettivo di illustrare il SGSI in termini di contesto, di obiettivi, di processi, di ruoli e di responsabilità rimandando a specifici documenti del sistema la trattazione approfondita dei singoli temi. Il SGSI, che si innesta all'interno dei processi già presidiati dall'Ente ed in coerenza con il modello organizzativo ed il sistema delle responsabilità da quest'ultimo adottato, è gestito all'interno dell'Area Innovazione e Servizi Operativi dall'Ufficio SGSI Governance.

Il Manuale SGSI è rivolto al personale di AdeR che ricopre i ruoli descritti nei successivi paragrafi e, in generale, a tutte le persone coinvolte nell'applicazione dell'SGSI e della norma ISO 27001.

IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il SGSI dell'Ente è stato ufficialmente avviato con l'emanazione del “Documento per la progressiva Implementazione del Sistema di Gestione della Sicurezza delle Informazioni

² La norma ISO 27001 è stata emanata dall'Organizzazione internazionale per la normazione (in inglese International Organization for Standardization, abbreviazione ISO) che è la più importante organizzazione a livello mondiale per la definizione di norme tecniche.

³ Accredia è l'Ente Unico nazionale di accreditamento designato dal governo italiano, in applicazione del Regolamento europeo 765/2008, ad attestare la competenza, l'indipendenza e l'imparzialità degli organismi di certificazione, ispezione e verifica, e dei laboratori di prova e taratura. Accredia è un'associazione riconosciuta che opera senza scopo di lucro, sotto la vigilanza del Ministero dello Sviluppo Economico.

(SGSI)"⁴. In tale documento, è delineato un approccio implementativo di tipo modulare che, a partire da un primo perimetro di analisi costituito dalle informazioni e dai dati trattati nell'ambito del Data Center, prevede una progressiva estensione a tutti i dati ed alle informazioni dell'Ente con l'obiettivo di rafforzare la protezione delle informazioni gestite per lo svolgimento delle attività istituzionali di riscossione nazionale e di amministrazione dei processi corporate.

Il SGSI e la norma ISO 27001, includendo tra i principi per la sicurezza delle informazioni, il rispetto della normativa vigente, dei contratti e delle convenzioni, sono importanti strumenti di supporto per l'Ente in termini di compliance, in particolare, rispetto alle seguenti norme: Regolamento generale sulla protezione dei dati n. 2016/679 (GDPR - General Data Protection Regulation); Provvedimenti del Garante per la protezione dei dati personali; Decreto Legislativo 7 marzo 2005, n. 82 "Codice di Amministrazione Digitale" (CAD); Circolare AgID del 18 aprile 2017, n. 2/2017 – Misure Minime di sicurezza per la PA; Piano nazionale per la protezione sicurezza cibernetica e la sicurezza informatica marzo 2017; Procedura Gestione degli incidenti di sicurezza CERT – MEF; Piano triennale per l'informatica nella Pubblica Amministrazione.

Dunque, curare la corretta evoluzione del SGSI è una chiara scelta strategica dell'Ente, adottata nella prospettiva di migliorare la capacità di proteggere le informazioni secondo le normative cogenti e a garanzia di tutte le Parti Interessate.

Il SGSI, definito secondo lo standard ISO 27001, è fondato sulla struttura denominata High Level Structure (HLS), ossia uno schema, elaborato dall'ISO (International Organization for Standardization), che ha l'obiettivo di definire una terminologia e una struttura di base, con parti di testo comuni, valide per tutte le norme dei sistemi di gestione proposti e certificabili dall'ISO. La struttura HLS del SGSI consente di definire puntualmente i requisiti e gli elementi necessari che il sistema di gestione deve avere, nonché di definire il percorso da intraprendere per conseguire, in modo stabile, misurabile e ripetibile, gli obiettivi di miglioramento ricercati.

Pertanto, il beneficio atteso derivante dall'adozione di un SGSI, strutturato secondo lo standard UNI EN CEI ISO IEC 27001:2017, è quello di garantire il controllo degli aspetti tecnologici, operativi e procedurali legati alla tutela delle informazioni, rafforzando ulteriormente la fiducia che le Parti Interessate ripongono nella capacità di AdeR di sviluppare ed erogare servizi in maniera efficiente e sicura. Il presente manuale ha lo scopo di indicare le scelte adottate dall'Ente per il corretto recepimento di ciascun punto dell'HLS previsto dalla norma ISO 27001, e di curare la diffusione dei contenuti della norma internazionale, delle metodologie e degli strumenti propri del SGSI a tutto il personale di AdeR.

⁴ Nota del Presidente protocollo n. 2017/2355014 del 22/12/2017 disponibile nella sezione della intranet aziendale relativa al SGSI.

Il SGSI, implementato secondo i requisiti indicati dalla norma ISO 27001, permette all'Ente di conseguire i seguenti obiettivi:

- garantire la gestione della sicurezza delle informazioni, in linea con le aspettative delle Parti Interessate, con gli obiettivi dell'Ente e con gli standard internazionali;
- normalizzare l'approccio alla gestione della sicurezza delle informazioni, ottimizzando e coordinando le risorse disponibili;
- creare un'organizzazione della sicurezza delle informazioni condivisa, documentata, organica, efficiente e capillare;
- consentire un miglioramento continuo del sistema di gestione della sicurezza delle informazioni;
- fornire metodologie, politiche e procedure di gestione

L'APPROCCIO PER PROCESSI

Il SGSI definisce ed attua un processo di gestione della sicurezza delle informazioni permanente che viene costantemente migliorato e mantenuto. Il principio del miglioramento continuo è garantito dalla realizzazione del modello PDCA (acronimo di Plan, Do, Check, Act, anche noto come ciclo di Deming). Tramite l'adozione di tale modello i risultati delle impostazioni e delle scelte di gestione vengono permanentemente monitorati e sottoposti a revisione in modo da garantire nel tempo la sicurezza del patrimonio informativo anche in presenza di eventuali cambiamenti dovuti a fattori esterni o interni all'organizzazione stessa dell'Ente.

La seguente figura rappresenta la schematizzazione del modello PDCA che, partendo dai requisiti e dalle aspettative delle Parti Interessate, attraverso le necessarie azioni e processi, contribuisce ad una corretta gestione della sicurezza delle informazioni.



Figura 1 - Modello PDCA del processo di gestione della sicurezza.

I processi sottesi dal SGSI tendono ad essere strutturati in maniera che:

- le finalità e le modalità di esecuzione del processo siano conosciute e comprese a tutti i livelli all'interno dell'organizzazione;

- le responsabilità siano stabilite chiaramente;
- la gestione della sicurezza sia integrata con gli altri processi come quelli di sviluppo, di gestione della qualità, dei cambiamenti e delle configurazioni, di assistenza agli utenti, di gestione operativa, di gestione del personale e di formazione;
- le procedure e i metodi utilizzati siano documentati, comunicati e misurati in termini di efficacia;
- le conoscenze e le competenze siano curate, mantenute e accresciute ai più alti livelli nella prospettiva di considerare la sicurezza come un bene e un contributo essenziale per il raggiungimento degli obiettivi di AdeR;
- la capacità nella gestione della sicurezza venga provata e valutata periodicamente.

Punto di forza del processo di miglioramento continuo attuato grazie al SGSI, è l'utilizzo di un approccio basato sulla analisi del rischio per la corretta identificazione e valutazione dei fattori di rischio e di opportunità. Lo scopo principale dell'approccio è quello di individuare, e così mettere in atto, delle azioni volte alla individuazione dei fattori che potrebbero creare criticità nei processi di sicurezza delle informazioni riducendone di conseguenza gli effetti indesiderati.

Tramite il SGSI basato sul modello PDCA e l'approccio di valutazione del rischio per la sicurezza delle informazioni, AdeR può controllare il raggiungimento degli obiettivi pianificati, indirizzare gli investimenti sulle iniziative di mitigazione del rischio e incrementare il livello di protezione dei dati e delle informazioni.

SEZIONE 1 – SCOPO E CAMPO DI APPLICAZIONE

Il piano di implementazione del sistema prevede una programmazione modulare e progressiva di attività che si estenderà per perimetri di analisi incrementali fino all'estensione del campo d'applicazione a tutto l'Ente ovvero a tutti i dati e le informazioni trattate. Per l'individuazione dei perimetri di analisi si è scelto un approccio di tipo "bottom-up" che, a partire dalle infrastrutture IT presenti nel Data Center, che primariamente influenzano la sicurezza delle informazioni, prosegue in una logica di incremento tecnologico fino alla copertura di tutti gli asset di natura strutturale, infrastrutturale, hardware e software in cui le informazioni dell'Ente transitano o vengono elaborate. Definito il layer tecnologico il sistema sarà ampliato rispetto alla copertura dei processi operativi impattati andando a valutare i rischi per la sicurezza delle informazioni inerenti ai processi istituzionali e corporate.

SEZIONE 2 - RIFERIMENTI NORMATIVI

2.1 NORMATIVA E DOCUMENTI DI RIFERIMENTO

NORMATIVA ISO

- [1] ISO/IEC 27001:2017 "INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS".
- [2] ISO/IEC 27000:2018 "INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — OVERVIEW AND VOCABULARY".
- [3] ISO/IEC 27002:2013 "INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS".

NORMATIVA COGENTE

- [4] Legge n. 547, 23.12.1993 – "Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica".
- [5] D. Lgs. n. 196 del 30 giugno 2003 – "Codice in materia di protezione dei dati personali" e successive modificazioni e integrazioni.
- [6] Legge n. 518, 29.12.1992 – "Attuazione della Direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".
- [7] Legge 20 maggio 1970, n. 300 Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento.
- [8] Provvedimento del Garante per la privacy del 27 novembre 2008, pubblicato sulla G.U. n. 300 del 24 dicembre 2008 – "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
- [9] D. Lgs 7 marzo 2005, n. 82 "Codice di Amministrazione Digitale" (CAD).
- [10] DPR 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".
- [11] Regolamento UE 2016/679 per la protezione dei dati personali (GDPR).
- [12] D. Lgs n. 101 del 10 agosto 2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 (GDPR)".
- [13] CCNL Contratto Nazionale Collettivo di Lavoro e Contratto integrativo del 28/03/2018.

NORMATIVA INTERNA

- [14] Codice Etico.
- [15] Modello di organizzazione, gestione e controllo ex decreto legislativo 8 giugno 2001, n. 231.
- [16] AdeR - Funzionigramma.
- [17] AdeR – Catalogo Servizi ICT e Operativi 2020 - Area Innovazione e Servizi Operativi.
- [18] Documenti in vigore e per quanto applicabili. Tra i principali:

- "DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI, PER GLI ACCESSI ALLE RISORSE E AI DATI DI AER"

- Circolare n. 39 "MISURE DI SICUREZZA ICT"

- Circolare n. 41 "ASSET MANAGEMENT IGI"
- Circolare n. 50 "IMPLEMENTAZIONE SERVIZI ICT"
- Manuale Unico n. 4 "LA SICUREZZA"
- Manuale Unico n. 8 "LE RISORSE UMANE"
- Sistema di protezione dati "PROCEDURA VIOLAZIONE DATI PERSONALI (DATA BREACH)"

DOCUMENTAZIONE SGSI

- [19] DIS_SGSI_Implementazione_SGSI - "Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)".
- [20] PGS_SGSI_Valutazione e trattamento del rischio - "Valutazione e trattamento del rischio".
- [21] PGS_SGSI_Audit Interni SGSI - "Audit interni di primo livello per l'SGSI".
- [22] PGS_SGSI_Gestione Non Conformità e Azioni Correttive - "Gestione Non Conformità e Azioni Correttive".

2.2 CORRELAZIONE TRA MANUALE E REQUISITI DELLA NORMA

Il manuale è stato redatto in conformità con la norma UNI EN CEI ISO IEC 27001: 2017.

Al fine di fornire al lettore un adeguato supporto nella comprensione del framework utilizzato dalla norma, nonché documentare la corretta adozione per le finalità di certificazione, è stata predisposta una matrice di correlazione tra la norma ISO 27001 ed il Manuale SGSI (Allegato 1).

SEZIONE 3 - TERMINI E DEFINIZIONI

Il Sistema di Gestione della Sicurezza delle Informazioni descritto in questo manuale tiene conto dei termini e delle definizioni riportati nella norma ISO 27000 [2].

Per favorire la chiara e corretta interpretazione delle prescrizioni riportate nel presente Manuale e facilitarne la comprensione si riportano di seguito gli acronimi ed i termini e le definizioni ritenute fondamentali:

3.1 SIGLE E ABBREVIAZIONI

- AISO – Area Innovazione e Servizi Operativi
- CAD – Codice dell'Amministrazione Digitale
- CERT – Computer Emergency Response Team
- DdA – Dichiarazione di Applicabilità
- MEF – Ministero Economia e Finanza
- PA – Pubblica Amministrazione

- PDCA – Plan-Do-Check-Act - Ciclo di Deming
- PTR – Piano di Trattamento del Rischio
- RACI (Responsible, Accountable, Consulted, and Informed) - Matrice per evidenziare l'assegnazione dei ruoli delle attività
- RAR – Rapporto Assessment del Rischio
- SGSI – Sistema di Gestione per la Sicurezza delle Informazioni
- SIF – Sistema Informativo della Fiscalità
- SNA – Sistema Normativo
- SPC – Sistema Pubblico di Connettività

3.2 TERMINI E DEFINIZIONI

Alta Direzione/ Verice: Persona o gruppo di persone che dirige e controlla un'organizzazione al massimo livello.

Analisi dei rischi: Utilizzo sistematico delle informazioni per identificare le fonti di rischio e per stimare il rischio.

Auditor interno di primo livello per il SGSI: Persona con le necessarie competenze per eseguire le verifiche ispettive di sicurezza per le informazioni.

Azione correttiva: Azione per eliminare la causa di una non conformità rilevata, o altre situazioni indesiderabili rilevate.

Bene/ Asset: Qualsiasi risorsa che abbia valore per l'organizzazione. L'asset primario per il SGSI è l'informazione.

Certificazione ISO 27001: La verifica e l'attestazione, condotta da enti terzi indipendenti e qualificati, che un'organizzazione, relativamente ad un certo ambito, ha realizzato un Sistema di Gestione della Sicurezza delle Informazioni conforme a quanto indicato nella norma ISO 27001.

Componente: Insieme di risorse che trattano l'informazione (la elaborano, la memorizzano o la comunicano) e/o ne influenzano la sicurezza. Il componente deve proteggere le informazioni contrastando le principali minacce con adeguate protezioni.

Controllo di sicurezza: Modalità di gestione del rischio, include Politiche, Procedure, Linee guida, strutture organizzative amministrative, tecniche, gestionali o legali.

Dichiarazione di applicabilità (DdA): Dichiarazione documentata che descrive gli obiettivi dei controlli ed i controlli che sono importanti ed applicabili nell'ambito del SGSI in base ai risultati della valutazione e del trattamento del rischio.

Disponibilità: Garanzia che gli utenti autorizzati abbiano accesso alle informazioni e ai beni associati, quando richiesto.

Evento di sicurezza: Circostanza identificata dello stato di un sistema, servizio o rete che indica una possibile violazione della politica per la sicurezza delle informazioni o una carenza nelle misure di protezione, o una situazione sconosciuta che può essere rilevante per la sicurezza.

Fornitore: Organizzazione o persona che fornisce un prodotto/servizio all'Ente.

Incidente di sicurezza: Singolo evento o serie di eventi di sicurezza delle informazioni, indesiderati o inaspettati, che ha una significativa probabilità di compromettere l'operatività di un sistema informativo e di minacciare la sicurezza delle informazioni.

Informazione: L'informazione è costituita da dati con annesso significato a cui l'organizzazione attribuisce un valore ai fini del conseguimento della propria missione.

Integrità: Salvaguardia dell'accuratezza e della completezza dell'informazione e dei metodi di elaborazione.

Miglioramento continuo: Attività ricorrente mirata ad accrescere la capacità del SGSI di soddisfare i requisiti per la sicurezza delle informazioni.

Modello PDCA: Modello di un sistema di gestione teso a soddisfare i requisiti richiesti dalle Parti Interessate migliorandosi continuamente. Il modello prevede quattro fasi: pianificazione (Plan), attuazione (Do), controllo (Check), miglioramento (Act).

Non conformità: Mancato soddisfacimento di un requisito.

Obiettivi per la sicurezza delle informazioni: Risultati che si vogliono raggiungere implementando il Sistema per la Sicurezza delle Informazioni.

Parti Interessate/ Stakeholder: Soggetti interni o esterni all'organizzazione, con interessi ed esigenze diversi, in grado di influenzare le scelte e i comportamenti dell'organizzazione di condizionarne il successo.

Perimetro: Ambito in cui è suddivisa AdeR ai fini della gestione della sicurezza delle informazioni.

Politica per la sicurezza delle informazioni: Orientamenti ed indirizzi generali di una organizzazione espressi in modo formale dall'alta direzione.

Requisito: Esigenza o aspettativa per la sicurezza delle informazioni che può essere espressa dalle Parti Interessate, generalmente implicita o contingente.

Riesame: Attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia dell'oggetto del riesame a conseguire gli obiettivi stabiliti.

Riservatezza: Garanzia che un'informazione sia accessibile solo a chi è autorizzato a farlo

Sicurezza dell'informazione: Protezione della riservatezza, dell'integrità e della disponibilità dell'informazione.

Sistema per la Gestione della Sicurezza delle Informazioni (SGSI): Modello per stabilire, attuare, gestire, controllare, revisionare, riadattare e migliorare le protezioni del patrimonio informativo al fine di raggiungere gli obiettivi di business. Il modello si basa sulla valutazione dei rischi e sui livelli di accettazione del rischio dell'organizzazione ed è disegnato per trattare e gestire efficacemente i rischi.

Valutazione del rischio: Insieme dei processi di analisi e misurazione del rischio.

SEZIONE 4 -CONTESTO DELL'ORGANIZZAZIONE

4.1 COMPRENDERE L'ORGANIZZAZIONE ED IL SUO CONTESTO

Le strutture di AdeR, in coerenza con le attribuzioni di responsabilità previste nel funzionigramma aziendale, concorrono ad assicurare l'efficiente ed efficace realizzazione degli obiettivi corporate e degli obiettivi istituzionali connessi alla riscossione dei tributi e, allo scopo, effettuano il trattamento di informazioni relative a contribuenti, personale interno ed esterno all'Ente, fornitori e altri Enti e Istituzioni. Le informazioni trattate sono adeguatamente protette a garanzia dei requisiti di riservatezza, integrità e disponibilità ed i trattamenti dei dati personali sono svolti nel pieno rispetto del Regolamento UE 2016/679 e del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", modificato dal D. Lgs. n. 101/2018.

L'Area ISO (Innovazione e Servizi Operativi) ha un ruolo centrale nel presidio dei rischi connessi alla sicurezza delle informazioni gestite tramite Servizi ICT, con particolare riferimento a quelle trattate nel Data Center, che di fatto costituiscono l'intero patrimonio informativo dell'Ente. Le attività condotte sono svolte in coerenza con le strategie e le decisioni del Vertice aziendale e con il complessivo governo delle risorse, al fine di garantire l'efficacia e l'efficienza dei sistemi, delle applicazioni, delle infrastrutture e dei servizi erogati per il regolare funzionamento dell'Ente e per il raggiungimento degli obiettivi di volta in volta individuati.

4.2 ESIGENZE ED ASPETTATIVE DELLE PARTI INTERESSATE

Le Parti Interessate alla sicurezza delle informazioni gestite da AdeR sono il Ministero dell'Economia e delle Finanze (MEF), per le funzioni di indirizzo e vigilanza sull'attività di AdeR e l'Agenzia delle Entrate, titolare dell'esercizio della funzione di riscossione nazionale, svolta da AdeR in qualità di ente strumentale. Nell'ambito delle Parti Interessate sono poi da annoverare il Vertice e i dipendenti di AdeR, gli Enti Impositori, i contribuenti, i Fornitori, le Autorità e le Istituzioni (es. Autorità del Garante per la protezione dei dati personali, AgID, ecc.).

In termini generali, secondo quanto previsto dalla normativa ISO 27001, le Parti Interessate hanno come aspettativa che il SGSI di AdeR provveda a garantire la sicurezza delle informazioni, mediante lo svolgimento di determinate attività contenute in specifici "Requisiti". Detti Requisiti sono costituiti da leggi e provvedimenti di legge, regolamenti, convenzioni, contratti, normativa interna (circolari, procedure e documenti dell'Ente), nonché dalla stessa normativa ISO 27001.

I Requisiti principali sono i seguenti:

- **Requisiti cogenti (Normativa esterna):**
 - Regolamento generale sulla protezione dei dati n. 2016/679, meglio noto con la sigla GDPR (General Data Protection Regulation);
 - Provvedimenti del Garante per la privacy in tema di sicurezza delle informazioni; per es.: il provvedimento del 27 novembre 2008, pubblicato sulla G.U. n. 300 del 24 dicembre 2008 – "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.;
 - Decreto Legislativo 7 marzo 2005, n. 82 "Codice di Amministrazione Digitale" (CAD) in materia di materia di documentazione amministrativa e s.m.i.;
 - Circolare AgID del 18 aprile 2017, n. 2/2017 – Misure Minime di sicurezza per la P.A.;
 - Piano triennale per l'informatica nella Pubblica Amministrazione – 2018/2020;
 - Piano nazionale per la protezione sicurezza cibernetica e la sicurezza informatica marzo 2017;
 - Procedura Gestione degli incidenti di sicurezza CERT – MEF.
- **Requisiti contrattuali (Accordi/Contratti):** contratti, accordi e convenzioni stipulati con Agenzia delle Entrate, Enti Impositori e fornitori di servizi che stabiliscono i Livelli di Servizio attesi anche per aspetti di sicurezza quali per esempio la disponibilità dei servizi (espressi sistematicamente nei documenti dispositivi del Sistema Normativo Aziendale -SNA- e nel Catalogo Servizi ICT pubblicato sulla Intranet). In tale contesto, vanno anche considerati gli accordi che scaturiscono da Organismi come il SIF (Sistema Integrato della Fiscalità), il CERT –MEF e altri a cui AdeR partecipa insieme alle agenzie fiscali, e alla Sogei.
- **Normativa interna di AdeR:**
 - Codice Etico;
 - Modello di organizzazione, gestione e controllo ex Decreto Legislativo 8 giugno 2001, n. 231;
 - Funzionigramma dell'Ente;
 - Modello Organizzativo dell'Ente;

- Documenti dispositivi del Sistema Normativo Aziendale (SNA) in vigore per quanto applicabili ed emanati dalle strutture deputate alle attività e funzioni descritte;
- “Documento per la progressiva implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI)”;
- Manuale SGSI – “Manuale per la gestione della sicurezza delle informazioni”;
- Circolare n. 39 “Misure di sicurezza”;
- “Disciplinare per l'utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati di AeR”.

• **Norma UNI CEI EN ISO IEC 27001:2017 (ISO 27001)**

Nella tabella che segue sono indicate le Parti Interessate (Interne ed Esterne) e le attività attese che il SGSI di AdeR deve svolgere per la soddisfazione di alcuni dei Requisiti più rilevanti.

Parti Interessate		Requisiti	Aspettative
Interne	Vertice di AdeR	Privacy	Garantire la protezione dei dati personali nella conduzione delle attività di riscossione e corporate dell'Ente.
		Requisiti AgID	Implementare, gestire e migliorare le adeguate misure di sicurezza sulle informazioni per proteggere le attività mission critical di AdeR e gli aspetti reputazionali.
		ISO27001	Operare sempre entro livelli accettabili di rischi per la sicurezza delle informazioni.
		ISO27001	Definire un quadro di riferimento per il governo della sicurezza delle informazioni in termini di requisiti, processi e responsabilità.
	Dipendenti di AdeR	Privacy	Trattare i dati personali dei dipendenti in conformità alle norme vigenti.
		ISO27001	Ricevere una formazione sulla sicurezza dell'informazione adeguata alla mansione.
		CCNL	Trattare i dati personali dei dipendenti nel rispetto di quanto previsto dal CCNL e in attuazione dello stesso.
	MEF e Agenzia delle Entrate	Normativa di Riscossione	Garantire l'esercizio dell'attività di riscossione in conformità alle norme vigenti.
		Privacy e Requisiti AgID	Salvaguardare il patrimonio informativo gestito dall'Ente.
Esterne	Enti Impositori	Convenzioni e Contratti	Trattare le informazioni in linea con gli accordi stabiliti.
	Contribuenti	Privacy	Trattare i dati personali dei contribuenti in conformità alle norme vigenti.
		ISO27001	Trattare le informazioni dei contribuenti garantendo la salvaguardia dei principi di riservatezza, integrità e disponibilità.

Parti Interessate	Requisiti	Aspettative
Fornitori (di tecnologia e servizi di supporto)	Convenzioni e Contratti	Gestire Asset e Infrastrutture nel rispetto degli SLA. Assicurare nel trasferimento e trattamento delle informazioni nel rispetto delle misure di protezione stabilite nei contratti in essere.
CERT- MEF	Requisiti CERT	Classificare e pianificare la risposta agli Incidenti di Sicurezza Informatica (IRP Incident Response Planning) secondo il processo indicato da CERT MEF. Eseguire l'attività di valutazione, per l'applicazione delle remediation in tema di sicurezza, indicate tramite gli appositi bollettini emanati dal CERT MEF
Istituzioni	Rapporti con le Istituzioni	Gestire le attività Istituzionali nel rispetto delle norme vigenti.
	Provvedimenti delle Authority	Adeguare i processi di gestione alle direttive emanate da Autorità ed altre istituzioni, per es. AgID, Garante per la protezione dei dati personali, ecc.

Ai fini della gestione del SGSI, sulla base del funzionigramma, sono identificabili le seguenti relazioni principali tra ruoli SGSI e strutture organizzative dell'Ente.

Struttura organizzativa	Finalità della relazione	Modalità di interfaccia
Direzione Tecnologie e Innovazione	Progettazione e predisposizione dei servizi e delle infrastrutture tecnologiche rispondenti ai requisiti di sicurezza delle informazioni.	L'implementazione e la gestione dei Sistemi e dei Servizi IT o l'evoluzione di quelli presenti è curata dal Settore Esercizio Sistemi ICT. Il SGSI richiede il rispetto dei principi e delle norme di sicurezza, nell'implementazione, nella gestione e nell'evoluzione dei sistemi, dei servizi e delle infrastrutture IT.
Direzione Affari Legali	Definizione delle clausole contrattuali per la garanzia della sicurezza delle informazioni nei rapporti con i fornitori.	L'implementazione del SGSI ha effetti sulle Relazioni con i fornitori per la diffusione della sicurezza delle informazioni e nella gestione dell'erogazione dei servizi dei fornitori (Controlli 15 Annex A ISO 27001).
Direzione Internal Audit	Condivisione della documentazione degli audit condotti dall'ufficio SGSI Governance.	Il Programma di audit annuale è condiviso con le strutture di Internal Audit per creare sinergie e condividere esiti e aspetti rilevati.
Direzione Risorse Umane	Disporre del personale e delle competenze necessarie	Il Responsabile SGSI predispone annualmente un piano di esigenze e requisiti connessi allo sviluppo e mantenimento del Sistema, esplicitando le esigenze di formazione in materia di sicurezza dell'informazione delle risorse di AdeR.

Struttura organizzativa	Finalità della relazione	Modalità di interfaccia
		Il piano viene condiviso e concordato con Risorse Umane che provvede all'organizzazione delle modalità necessarie alla sua attuazione. Il gestore SGSI supporta il Responsabile del SGSI nella definizione dei contenuti e nella migliore diffusione degli approcci previsti dalla norma ISO27001.
Direzione Approvvigionamenti e Logistica	Disporre di locali dotati delle necessarie caratteristiche di sicurezza.	Il SGSI richiede il rispetto di regole di sicurezza anche per l'accesso ai locali delle due sedi del Data Center (primaria e secondaria) che accolgono le tecnologie ICT ed i servizi tecnici annessi. Inoltre, richiede il rispetto delle regole vigenti per la implementazione e gestione dei sistemi e degli apparati di protezione fisica del Data Center (anti incendio, condizionamento, anti intrusione, gruppi elettrogeni, ecc.)
OdV (Organismo di vigilanza)	Coinvolgimento nelle questioni inerenti possibili violazioni di leggi cogenti che portano a condanne penali.	In tutti i casi nei quali sono rilevati possibili reati connessi al trattamento di dati e informazioni.
DPO (Data Protection Officer)	Coinvolgimento nelle questioni inerenti il trattamento dei dati personali di cui AdeR è Titolare.	In tutti i casi nei quali sono rilevati impatti sui dati personali è interessato il DPO per le questioni di competenza.

Relativamente alle interdipendenze e interfacce esterne, per la gestione e la manutenzione di alcuni servizi e delle infrastrutture del Data Center, AdeR ha stipulato specifici contratti con fornitori di servizi. Di seguito si riporta l'elenco delle categorie dei servizi contrattualizzati rilevanti per la sicurezza delle informazioni, rinviando al contenuto di ciascun contratto per quanto riguarda le specifiche clausole e/o condizioni ed ogni altra informazione di dettaglio.

Pulizia/ Derattizzazione,

Manutenzione locali,

Anti incendio,

Video Sorveglianza,

Anti intrusione,

Anti allagamento,

Impianto elettrico (cablaggi di rete),

Servizi di connettività (SPC e altre reti,)

Manutenzione HW,

Manutenzione SW,

Servizi CERT-MEF (vulnerability assessment: bollettini).

Il Campo di Applicazione rientra tra le informazioni documentate che l'Ente deve mantenere per istituire il proprio SGSI ed il suo aggiornamento.

4.3 DOCUMENTI DEL SGSI

In rispondenza a precisi requisiti documentali richiesti dalla norma ISO 27001 ed al fine di garantire una adeguata efficacia del SGSI, sono stati predisposti i seguenti specifici documenti, le c.d. informazioni documentate SGSI, pubblicati nella sezione "Compliance – SGSI" della Intranet di Agenzia:

- Documento SGSI: Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI).
- SGSI – Manuale.
- SGSI – Valutazione e trattamento del rischio di sicurezza delle informazioni.
- SGSI - Gestione delle non conformità e azioni correttive.
- SGSI - Audit interni di primo livello.

La documentazione generale a supporto dell'operatività dei processi è invece gestita attraverso lo SNA. Le circolari, le procedure e le istruzioni di lavoro necessarie per supportare l'attuazione di tutti i processi (compresi quelli inerenti alla sicurezza delle informazioni) sono contenute nell'apposita sezione intranet "Normativa/Sistema Normativo Agenzia" dove è possibile consultare la documentazione anche attraverso appositi filtri rispetto alla tipologia (circolare/direttive, Note informative, etc.) o al tipo di processo (governo, supporto, operativo). La manutenzione del sistema Normativo Aziendale è gestita dalla Direzione Organizzazione e Processi.

SEZIONE 5- LA LEADERSHIP

5.1 LEADERSHIP E IMPEGNO

L'Ente si impegna a realizzare, attuare e migliorare il proprio SGSI in conformità ai migliori standard internazionali, al fine di supportare lo svolgimento della propria missione istituzionale. AdeR intende concretizzare l'impegno nello sviluppo del proprio SGSI in conformità alla norma UNI EN CEI ISO IEC 27001:2017, facendone un elemento chiave per

garantire la protezione delle informazioni, in termini di rispetto dei requisiti di riservatezza, integrità e disponibilità, trattate nei suoi processi di funzionamento.

Coerentemente con il sistema di certificazione, l'impegno a mantenere e migliorare il SGSI viene presidiato dal Vertice dell'Ente al quale sono forniti stati di avanzamento ed evidenze dei risultati conseguiti. Il Vertice si impegna a realizzare e attuare il SGSI concorrendo al funzionamento efficiente ed efficace dello stesso.

In particolare, il Vertice di AdeR provvede a:

- adottare il Sistema di Gestione per la Sicurezza delle Informazioni;
- definire la struttura organizzativa formalizzando compiti e responsabilità per la gestione della sicurezza delle informazioni;
- comunicare al personale la rilevanza degli obiettivi, delle politiche, dei requisiti cogenti (leggi, regolamenti) in tema di sicurezza delle informazioni;
- stimolare il miglioramento continuo nella gestione della sicurezza delle informazioni;
- approvare le risultanze del riesame del SGSI.

Al fine di proteggere adeguatamente le informazioni, per il SGSI dell'Ente sono stati individuati specifici ruoli che concorrono nella comprensione e qualificazione dei requisiti di sicurezza.

5.2 POLITICA

La Politica SGSI, che costituisce parte integrante della documentazione del Sistema di Gestione per la Sicurezza delle Informazioni, inerente alle strategie implementate e gli obiettivi da conseguire coerenti con le aspettative delle Parti Interessate, è contenuta nel "Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)".

5.3 RUOLI, RESPONSABILITÀ E AUTORITÀ NELL'ORGANIZZAZIONE

L'organizzazione degli aspetti di gestione della sicurezza delle informazioni è garantita da due aree distinte di intervento:

- **pianificazione e coordinamento** della sicurezza con funzioni di indirizzo e vigilanza curata dal Gestore SGSI;
- **gestione operativa** dei servizi connessi all'attuazione della sicurezza ed alle funzioni di controllo, curata per competenza dalle strutture di AdeR o per esse dai Fornitori.

Tale livelli di intervento, sono attuati nel Sistema di Gestione della Sicurezza delle informazioni di AdeR introducendo ruoli e attività che, in linea con il modello organizzativo di AdeR, sono specificamente attribuiti alle strutture organizzative dell'Ente. Nella seguente figura è riportato lo schema adottato per l'organizzazione del SGSI:

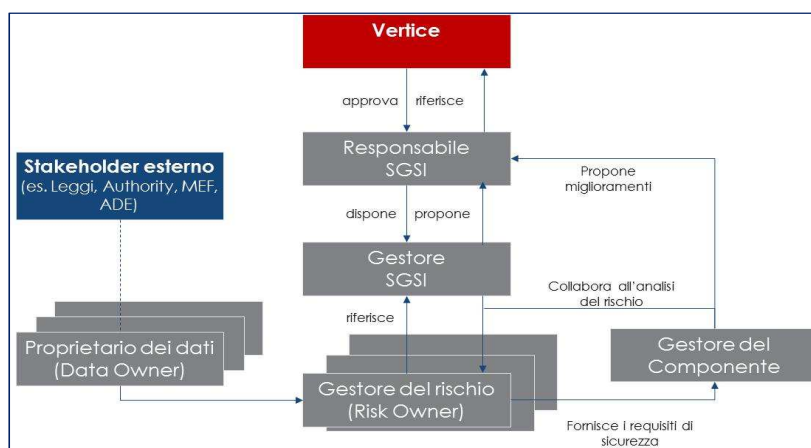


Figura 2 - Schema per l'organizzazione del SGSI

Di seguito per ciascun ruolo si riportano le specifiche attribuzioni spettanti in ambito AdeR.

RESPONSABILE SGSI

Il Responsabile SGSI deve:

- verificare l'applicazione del SGSI e il suo riesame periodico;
- definire e formalizzare i criteri di accettazione del rischio verificandone il rispetto delle esigenze in tema di sicurezza delle informazioni;
- valutare le prestazioni della sicurezza delle informazioni e l'efficacia del SGSI in termini di contenimento del rischio;
- definire gli obiettivi e i piani del SGSI da sottoporre all'approvazione del Vertice;
- indirizzare e supportare le iniziative di sicurezza delle informazioni;
- pianificare e garantire la disponibilità delle risorse necessarie per sviluppare, realizzare e rendere operativo il SGSI;
- garantire l'implementazione delle politiche generali di sicurezza delle informazioni;
- informare il Vertice sulle principali evidenze in materia di gestione dei rischi inerenti alla sicurezza delle informazioni;
- curare l'emanazione dei documenti del SGSI, nel rispetto della normativa vigente e previa condivisione con le competenti strutture dell'Ente.

Tale ruolo viene attribuito al Responsabile dell'Area Innovazione e Servizi Operativi.

GESTORE SGSI

Il Gestore del SGSI ha il compito di:

- garantire l'applicazione del SGSI e il suo riesame periodico;
- aggiornare il Responsabile del SGSI sui risultati degli Internal Security Audit, sull'andamento generale del SGSI e sulla pianificazione degli interventi previsti;
- gestire il sistema documentale del SGSI;

- tenere sotto controllo gli obiettivi e i piani del SGSI;
- proporre le azioni da intraprendere per il miglioramento della sicurezza delle informazioni e promuovere iniziative di sicurezza delle informazioni;
- supportare il dialogo tra le strutture che realizzano la gestione operativa del SGSI nella valutazione dei rischi e dei livelli di adeguatezza dei controlli di sicurezza previsti, in relazione alle modalità di trattamento dei dati e delle informazioni (c.d. componente);
- definire i requisiti del sistema di indicatori per il monitoraggio del SGSI, nonché raccogliere le informazioni utili al monitoraggio;
- riesaminare periodicamente i risultati del SGSI e analizzare la reportistica sugli incidenti di sicurezza, sugli indicatori di prestazione e sulle verifiche ispettive interne;
- sviluppare la cultura della sicurezza attraverso la promozione di formazione specifica per il personale.

Tale ruolo viene attribuito all'Ufficio SGSI Governance.

PROPRIETARIO DEI DATI (DATA OWNER)

Il Proprietario dei dati o Data Owner ha il compito di esprimere le necessità e le aspettative di sicurezza per le informazioni che gestisce tenendo in considerazione anche le normative vigenti, i contratti, le aspettative di terzi (contribuenti, Enti creditori, ecc.) e il contesto di riferimento.

Tale ruolo viene attribuito, in relazione alle attività assegnate nel modello organizzativo di AdeR, alle Strutture Centrali (Direzioni Centrali e Aree, per il tramite delle proprie articolazioni organizzative) owner dei processi ove sono trattati i dati e le informazioni, anche quali punti di riferimento per le attività svolte dalle Strutture Regionali.

GESTORE DEL RISCHIO (RISK OWNER)

Il Gestore del rischio o Risk Owner ha il compito di:

- raccogliere le aspettative di sicurezza del Proprietario dei dati in coerenza con le aspettative di contenimento del rischio;
- raccogliere le valutazioni sulle misure di sicurezza presenti o da prevedere da parte del Gestore del componente;
- analizzare le informazioni raccolte per concertare gli interventi sulle misure di sicurezza da realizzare anche tenendo conto dei criteri di accettazione dei rischi definiti dal responsabile del SGSI;
- monitorare e aggiornare le valutazioni di adeguatezza del trattamento dei rischi.

Tale ruolo viene attribuito, in relazione alle attività assegnate nel modello organizzativo di AdeR, alle Strutture di Demand and Delivery della Direzione Tecnologie e Innovazione.

GESTORE DEL COMPONENTE

Le tipologie di controllo da gestire al fine di mitigare i rischi di sicurezza dipendono dalle caratteristiche del trattamento effettuato (elaborazione, memorizzazione, comunicazione, ecc.) dei dati e delle informazioni. In particolare, le componenti che possono intervenire nel trattamento del dato e/o dell'informazione sono prevalentemente:

- A. Hardware (server, client, reti, ecc.)
- B. Software (applicazioni, sistemi operativi e sistemi di gestione)
- C. Logistica (locali fisici, impianti infrastrutturali, ecc.)
- D. Personale (competenze)

Ciascuna componente del trattamento presenta tipologie specifiche di minacce e di azioni di protezione da valutare. Il Gestore del componente ha il compito, con riferimento alla componente di competenza, di:

- valutare il livello di esposizione alle minacce definendo il grado di efficacia delle misure in essere;
- attivare le ulteriori misure necessarie alla riduzione del rischio concordate con il Gestore del rischio;
- assicurare l'effettivo funzionamento delle misure di sicurezza previste.

Tale ruolo viene attribuito alle strutture di AdeR in relazione alle attività assegnate nel modello organizzativo. In particolare, sono principalmente coinvolte:

- Direzione Tecnologie e Innovazione – Settore Esercizio Sistemi ICT (per le componenti A e B);
- Direzione Approvvigionamenti e Logistica – Settore Logistica Infrastrutture e Security (per la componente C);
- Direzione Risorse Umane – Settore Gestione Risorse Umane (per la componente D).

SEZIONE 6 – PIANIFICAZIONE

6.1 AZIONI PER AFFRONTARE RISCHI E OPPORTUNITÀ

La pianificazione delle attività operative del SGSI viene definita sulla base del rischio per la sicurezza delle informazioni.

Nell'ambito del SGSI è stato stabilito il processo di valutazione e trattamento del rischio illustrato nel documento: "PGS_SGSI_Valutazione e trattamento del rischio" [20].

VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

La valutazione del rischio adottata è di tipo qualitativo, si basa sui processi e criteri illustrati in termini generali nel documento "PGS_SGSI_Valutazione e trattamento del rischio" [20] e si articola nelle seguenti attività:

- Valutazione della criticità delle informazioni;

- Identificazione dei componenti e valutazione delle vulnerabilità e delle minacce;
- Valutazione dei controlli applicati ai componenti e della loro efficacia;
- Misurazione del rischio;
- Redazione Rapporto di Assessment del Rischio (RAR).

L'organizzazione deve conservare informazioni documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni.

TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

Il processo di trattamento del rischio è illustrato nel documento: "PGS_SGSI_Valutazione e trattamento del rischio" [20]. Il processo prevede le seguenti attività:

- la selezione delle adeguate opzioni per il trattamento del rischio;
- la redazione della "Dichiarazione di Applicabilità" che riporta i controlli necessari e le giustificazioni per l'inclusione, che siano attuati o meno, o per l'esclusione dei controlli dell'appendice A della norma 27001;
- la formulazione del piano di trattamento del rischio (PTR);
- l'accettazione del rischio residuo.

I criteri di accettazione del rischio sono indicati nel documento: "PGS_SGSI_Valutazione e trattamento del rischio" [20].

L'organizzazione deve conservare informazioni documentate sul processo di trattamento del rischio relativo alla sicurezza delle informazioni.

6.2 OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI

Il Gestore del SGSI predispone un "Piano annuale per la sicurezza delle informazioni". Il Piano viene presentato dal Responsabile del SGSI al Vertice di AdeR, quindi viene comunicato ai principali attori del SGSI.

Nel Piano sono indicati gli obiettivi del periodo e le attività previste per conseguire tali obiettivi con l'indicazione del Responsabile e dei contenuti dell'attività, delle risorse previste, dei tempi stimati e delle modalità di valutazione dei risultati.

Inoltre, nel Piano vengono indicati, gli obiettivi per l'audit di primo livello, per la formazione e per le misurazioni, nonché gli interventi per il miglioramento continuo dei controlli e dei relativi processi.

SEZIONE 7 – SUPPORTO

7.1 RISORSE

L'aspetto della disponibilità delle risorse viene trattato e registrato in specifici documenti quali il Piano per la sicurezza delle informazioni e nei verbali del Riesame di direzione. In particolare, viene curata:

- una pianificazione generale delle risorse;
- la coerenza tra pianificazione delle risorse in termini quantitativi e competenza/piani di formazione;
- la tempestività nella messa a disposizione delle risorse.

7.2 COMPETENZA

Per gli aspetti di addestramento e competenza viene messa in atto:

- la definizione delle competenze richieste per i ruoli relativi ai processi inerenti alla sicurezza;
- la definizione di azioni di formazione ed addestramento per assicurare la necessaria competenza attraverso la definizione di un piano di formazione;
- la verifica dell'efficacia della formazione effettuata.

7.3 CONSAPEVOLEZZA

I principi, le politiche e gli aspetti generali del SGSI vengono comunicati a tutto il personale affinché siano consapevoli dell'importanza del proprio contributo e delle implicazioni delle non conformità ai requisiti di sicurezza.

7.4 COMUNICAZIONE

Nelle procedure del SGSI vengono indicati i criteri di comunicazione delle risultanze delle varie attività anche con l'ausilio della matrice RACI (Responsible, Accountable, Consulted, and Informed). La comunicazione interna è gestita mediante:

- riunioni periodiche con i ruoli SGSI interessati che permettono il confronto sulle principali evidenze delle analisi e misurazioni del rischio;
- sezione dedicata all'interno della intranet aziendale nella quale sono disponibili tutti i documenti che compongono il SGSI (Manuale, Procedure, Registrazioni).

7.5 INFORMAZIONI DOCUMENTATE

Le informazioni documentate relative al Sistema di Gestione per la Sicurezza delle Informazioni dimostrano l'evidenza oggettiva di:

- attività eseguite;
- risultati ottenuti in termini di soddisfacimento di requisiti normativi, cogenti e interni, della norma;
- efficacia operativa.

Tali documenti, previsti dalla norma ISO 27001 e obbligatori, facilitano l'analisi del livello di sicurezza per le informazioni e permettono di ricavare dati di tendenza al fine di migliorare l'attuazione e l'efficacia del SGSI. In particolare, il Sistema di Gestione della Sicurezza delle Informazioni dell'Ente utilizza:

- le informazioni documentate richieste dalla Norma ISO 27001 per l'adeguata verifica dello standard;
- le informazioni documentate che sono ritenute utili ad avere una adeguata garanzia della protezione delle informazioni. Tra queste, vi sono istruzioni e prassi documentate a supporto dei processi operativi, nonché quelle che emergono come necessarie per effetto di analisi dei rischi/opportunità applicate ai processi.

Quindi, per informazioni documentate SGSI si possono intendere:

- 1) **documenti**, cioè informazioni documentate prodotte internamente che descrivono aspetti di carattere organizzativo, procedurale e operativo;
- 2) **registrazioni**, cioè informazioni documentate prodotte internamente che forniscono evidenza del funzionamento del SGSI e delle relative risultanze;
- 3) informazioni documentate di **origine esterna**.

I documenti SGSI seguono un ciclo di vita che comprende le seguenti fasi: redazione, verifica e approvazione, emissione e divulgazione, modifica, conservazione. Il formato del template prevede almeno le seguenti informazioni caratteristiche del documento: Titolo del documento, Identificativo del documento, Versione.

Le registrazioni sono informazioni documentate che forniscono traccia del funzionamento del SGSI raccogliendo dati su eventi o stati/situazioni. Le registrazioni pertanto non sono soggette ai cicli di approvazione, emissione e revisione e possono essere effettuate in diverse modalità, con diversi prodotti, utilizzando diversi tipi di supporto (cartaceo, tecnologico ecc.).

Le registrazioni, così come i documenti di origine esterna, devono essere identificate e conservate da parte del Gestore SGSI che provvede anche a garantirne l'integrità e riservatezza.

Il sistema documentale è articolato in due livelli: un Livello Generale per le informazioni documentate valide per tutto il SGSI, ed un Livello Componente per le informazioni documentate specifiche dei singoli componenti che progressivamente vengono analizzati.

Per i due livelli del SGSI sono previste le seguenti tipologie di informazioni documentate:

- Livello Generale
 - **DIS**: Documenti di Indirizzo SGSI
 - **PGS**: Procedure generali SGSI
 - **IDS**: Informazioni documentate per il SGSI
 - **MGS**: Modulistica SGSI
 - **RGS**: Registrazioni SGSI
- Livello Componente (per ogni componente che viene incluso nel SGSI: es. hardware, software, infrastrutturale)
 - **IDP**: Informazioni SGSI documentate a livello di componente
 - **RPS**: Registrazioni SGSI a livello di componente (es. attività operativa, processo volto alla sicurezza delle informazioni)

Ai documenti inerenti al SGSI viene attribuito un codice documento che risponde ai seguenti criteri:

- tre caratteri alfabetici "XXX" che indicano la tipologia di informazioni documentate rispetto i precedenti livelli;
- la sigla SGSI;
- un titolo sintetico;
- ove applicabile, l'identificativo della versione (es. v10, v11).

Tutti i documenti prodotti nell'ambito SGSI sono conservati e classificati dal Gestore SGSI in un apposito documentale.

I documenti di indirizzo SGSI (DIS) sono predisposti dal Gestore SGSI con il supporto delle strutture di AdeR coinvolte. I documenti sono verificati e approvati dal Responsabile SGSI. È cura del Gestore SGSI supportare la fase di emissione e divulgazione e provvedere alla conservazione.

Le procedure generali SGSI (PSG), le Informazioni documentate per il SGSI (IDS) prevedono un iter analogo al precedente con approvazione da parte del Responsabile SGSI.

La modulistica (MGS) e le registrazioni (RGS) SGSI sono totalmente a cura del Gestore SGSI: dalla fase di redazione alla fase di conservazione.

I documenti a livello di componente (IDP e RPS) sono definiti e prodotti dai referenti del Gestore del componente (esempio registrazioni accessi fisici, lista hardware) e prevedono il coinvolgimento del Gestore SGSI sia per la fase di supporto alla redazione che di accettazione.

Per la documentazione di origine esterna il Gestore SGSI provvede alla conservazione.

Le informazioni documentate obbligatorie per un SGSI conforme alla ISO 27001 sono le seguenti:

- Il campo di applicazione deve essere disponibile come insieme di informazioni documentate.
- La politica per la sicurezza delle informazioni deve essere disponibile come insieme di informazioni documentate.
- Le informazioni documentate sul processo di valutazione del rischio relativo alla sicurezza delle informazioni.
- Le informazioni documentate sul processo di trattamento del rischio relativo alla sicurezza delle informazioni.
- Le informazioni documentate sugli obiettivi per la sicurezza delle informazioni.
- Le informazioni documentate quale evidenza delle competenze.
- Per la pianificazione e i controlli operativi, le informazioni documentate nella misura necessaria ad avere fiducia che i processi siano stati eseguiti come pianificato.
- Le informazioni documentate sui risultati delle valutazioni del rischio relativo alla sicurezza delle informazioni.
- Le informazioni documentate sui risultati del trattamento del rischio relativo alla sicurezza delle informazioni.
- Le informazioni documentate quale evidenza dei risultati dei monitoraggi e delle misurazioni.
- Le informazioni documentate quale evidenza dell'attuazione del programma di audit e dei risultati di audit.
- Le informazioni documentate quale evidenza dei risultati dei riesami di direzione.
- Le informazioni documentate quale evidenza:
 - o della natura delle non conformità e ogni successiva azione intrapresa, e
 - o dei risultati di ogni azione correttiva.

SEZIONE 8 – ATTIVITÀ OPERATIVE

8.1 PIANIFICAZIONE E CONTROLLI OPERATIVI

L'attività di attuazione e conduzione del SGSI prevede di rendere operativo il Piano annuale per la sicurezza delle informazioni.

Il Gestore del SGSI tiene sotto controllo i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto le azioni previste nel Piano annuale per la sicurezza delle informazioni verificando l'allineamento con gli obiettivi stabiliti.

I controlli operativi sono verificati anche mediante la valutazione documenti di origine esterna forniti dai Gestori dei componenti per l'attestazione delle misure di sicurezza attuate.

8.2 VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

Il Gestore del SGSI attiva l'esecuzione delle valutazioni del rischio per l'ambito previsto nel Piano annuale per la sicurezza delle informazioni.

La procedura e le modalità per la conduzione della valutazione sono riportate nel documento "PGS_SGSI_Valutazione e trattamento del rischio" [20], che descrive anche il processo di accettazione del rischio, basato sui criteri di accettabilità stabiliti per il SGSI dal Responsabile del SGSI.

8.3 TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI

Il Gestore del SGSI attiva l'esecuzione del trattamento del rischio per i servizi previsti nel Piano annuale per la sicurezza delle informazioni, per i quali è stata effettuata la valutazione del rischio.

La procedura e le modalità per la conduzione del trattamento del rischio e dell'accettazione del rischio residuo sono riportate nel documento: "PGS_SGSI_Valutazione e trattamento del rischio" [20].

SEZIONE 9 – VALUTAZIONE DELLE PRESTAZIONI

9.1 MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE

L'attività di monitoraggio e riesame del SGSI consiste nel valutare e misurare le prestazioni del SGSI a fronte della politica, degli obiettivi e delle esperienze pratiche e, quindi, riportare i risultati al Vertice dell'Ente per il riesame.

Le principali attività riguardanti tale fase sono il monitoraggio del sistema attraverso le misure di efficacia dei controlli, la conduzione di Audit di primo livello, la gestione degli incidenti di sicurezza, il riesame delle valutazioni del rischio e il Riesame di direzione.

Gli obiettivi strategici del SGSI sono perseguiti tramite l'utilizzo di un approccio di tipo top-down secondo il quale vengono scomposti in obiettivi di sicurezza che sono realizzati mediante il compimento di specifiche attività e azioni. Queste ultime sono identificate in modo tale che risultino significative e misurabili, che possano essere attribuite in termini di responsabilità e verificate rispetto a dei valori target di riferimento.

La misurazione delle azioni, mediante l'introduzione di opportuni costrutti di misura, permette di valutare il raggiungimento degli obiettivi di sicurezza che, se adeguatamente definiti, consentono di valutare il soddisfacimento degli obiettivi strategici del SGSI. Nella seguente Figura si fornisce una rappresentazione di tale scomposizione.



Figura 2: Obiettivi strategici e obiettivi di sicurezza.

In base a quanto premesso, gli obiettivi di sicurezza sono stati identificati al fine di consentire la misurazione degli obiettivi strategici e, pertanto, sono stati definiti secondo i seguenti criteri e opportunità:

1. Gli obiettivi sono connessi ad uno o più dei requisiti di sicurezza delle informazioni del SGSI cioè, riservatezza, integrità e disponibilità.
2. Gli obiettivi sono misurabili o cosiddetti SMART, ossia l'obiettivo deve essere Specifico (tale che risulti chiaro e comprensibile per chi deve realizzarlo), Misurabile (in modo che sia quantificabile il risultato ottenuto, facilitandone la valutazione), Accessibile (tale che sia effettivamente realizzabile, date le risorse a disposizione), Rilevante (tale che risponda effettivamente alle strategie e in ultima istanza alle aspettative degli stakeholder) e Temporalmente definito.
3. Gli obiettivi sono significativi per un SGSI, quali ad esempio connessi alla gestione degli incidenti o al controllo accessi fisici, in generale riconducibili ai requisiti e ai controlli della norma (per questi ultimi la ISO 27002 individua delle linee guida che definiscono proprio obiettivi di sicurezza).
4. Per ogni obiettivo strategico, è definito un numero di obiettivi perseguibile e attribuibile in termini di responsabilità che consenta al contempo di avere una misura dell'efficacia delle azioni attuate per la sicurezza delle informazioni.

La registrazione degli indicatori e dei dati misurati avviene, come detto, utilizzando opportuni costrutti di misura che, a partire dalle misure base, permettono di valutare il raggiungimento degli obiettivi di sicurezza. I costrutti sono conservati dal Gestore SGSI e sono sempre condivisi con i responsabili delle misurazioni che rappresentano coloro che hanno competenza e disponibilità dei dati oggetto delle misure.

I responsabili delle misurazioni raccolgono, con la frequenza prevista o comunque su richiesta, i dati primari relativi agli indicatori da monitorare e li trasmettono all'Ufficio SGSI Governance in qualità di Gestore SGSI. I dati richiesti, laddove disponibili in modalità stabile e ripetibile, possono essere oggetto di estrazione dai sistemi informativi da parte del medesimo ufficio.

Il Gestore SGSI avvalendosi se necessario del supporto delle strutture interessate, effettua le seguenti operazioni:

- elabora i dati primari, ne ottiene le misurazioni di sintesi e ne effettua opportuna registrazione e conservazione;
- effettua una interpretazione dei dati a fini valutativi e predispone le necessarie analisi.

Le analisi di cui sopra costituiscono elemento di ingresso per il Riesame di direzione e possono essere origine di azioni correttive o migliorative.

9.1.1 DEFINIZIONI

Di seguito si riportano alcune definizioni sintetiche relative ai principali elementi utilizzati nel processo di misurazione dei controlli di sicurezza e che definiscono i cosiddetti costrutti di misura.

- Obiettivo di misurazione: valutazione del livello di attuazione/efficacia di un controllo di sicurezza;
- Oggetto di misurazione: controllo di sicurezza che si vuole misurare;
- Misura base: la misura più semplice utilizzata per misurare un attributo dell'oggetto di misurazione.
- Metodo di misurazione: criterio di utilizzo della misura base
- Misura derivata: funzione (combinazione /aggregazione) di due o più misure base, ottenuta applicando una "funzione di misurazione" alle misure base.
- Indicatore: misura ottenuta applicando un "modello analitico" a misure base e/o derivate e combinandole con criteri decisionali.

9.2 AUDIT DI PRIMO LIVELLO

L'Ufficio SGSI Governance definisce e attua annualmente un Programma di audit interni SGSI di primo livello volto ad accertare che le attività sottoposte al SGSI vengano effettuate in conformità ai requisiti della norma ISO 27001 e a quelli stabiliti dall'organizzazione stessa.

A tal fine, è stata predisposta la procedura "PSG_SGSI_Audit interni per il SGSI" [21] che definisce le responsabilità ed i criteri inerenti:

- Definizione del Programma di Audit;
- Pianificazione degli Audit;
- Preparazione degli Audit;

- Conduzione degli Audit;
- Chiusura degli Audit;
- Azioni successive agli Audit;
- Valutazione dei risultati.

La pianificazione degli audit interni SGSI viene attuata in modo da coprire, con criteri di campionamento, le attività operative e i processi che influenzano la sicurezza delle informazioni nel campo di applicazione del sistema, con approfondimenti diversificati in rapporto all'impatto degli stessi sulla sicurezza. Affinché gli audit siano efficaci:

- è predisposto un piano di Audit tale da individuare i punti chiave del sistema e seguirne l'evoluzione nel tempo;
- sono definiti i contenuti da sottoporre a verifica per ogni singola area e i criteri di oggettivazione dei risultati;
- vengono formalizzati gli esiti;
- vengono analizzati e valutati i risultati delle verifiche pianificando le eventuali azioni correttive o di miglioramento.

Il programma annuale di audit SGSI, approvato dal Responsabile SGSI, viene comunicato alla Direzione Internal Audit alla quale viene fornita anche opportuna documentazione di sintesi dei risultati ottenuti.

Tutta la documentazione prodotta viene conservata dal Gestore SGSI in modo che sia sempre disponibile per approfondimenti.

Gli esiti e le informazioni emerse dagli internal audit SGSI, oltre a innescare azioni correttive immediate e mirate alle singole aree, costituiscono lo strumento fondamentale per il Riesame del Sistema.

Nel corso del Riesame di direzione il Vertice dell'Ente verifica le attività svolte per l'attuazione, il mantenimento e lo sviluppo del SGSI. Nel corso del Riesame di direzione, il Vertice può indicare eventuali e specifiche iniziative da adottare per il miglioramento del Sistema di Gestione.

9.3 RIESAME DI DIREZIONE

Il Riesame di direzione per il SGSI viene effettuato, annualmente o in base alle necessità, dal Responsabile del SGSI congiuntamente al Gestore SGSI e riportato mediante la relazione annuale al Vertice dell'Ente.

L'obiettivo del Riesame è di:

- assicurare l'idoneità, l'adeguatezza e l'efficacia nel tempo del SGSI in termini di processi, organizzazione e risorse;
- verificare il livello di sicurezza raggiunto;
- rivedere le politiche di sicurezza.

Gli elementi in ingresso al Riesame sono:

- Stato delle azioni derivanti dai precedenti riesami di direzione.
- Cambiamenti dei fattori esterni e interni che hanno attinenza con il SGSI.
- Informazioni di ritorno sulle prestazioni del SGSI:
 - Risultati degli audit interni o esterni da parte di enti terzi.
 - Andamento delle NC e AC. Stato delle azioni correttive o preventive.
 - Risultati del monitoraggio e della misurazione.
 - Risultati del raggiungimento degli obiettivi di sicurezza.
- Informazione di ritorno dalle parti interessate.
 - Informazioni derivanti dalla Valutazione del rischio ad esempio Revisione della valutazione del rischio, integrazione Vulnerabilità e minacce non correttamente individuate nella precedente analisi del rischio, Miglioramento: Piano di trattamento del rischio.
- Opportunità di miglioramento.
 - Modifiche a requisiti definiti alla base del processo di sviluppo del SGSI.
 - Revisione della politica della sicurezza delle informazioni.

Gli elementi in uscita al Riesame sono:

- miglioramento dell'efficacia del SGSI;
- aggiornamento dei piani di valutazione e trattamento dei rischi;
- modifiche a procedure e controlli che hanno effetto sulla sicurezza delle informazioni;
- miglioramento del metodo di misurazione dell'efficacia dei controlli.

L'esito del Riesame viene documentato in un verbale riunione ed è conservato dal Responsabile del SGSI. Il Responsabile del SGSI provvede, se ritenuto utile, a comunicare alle Parti Interessate le azioni intraprese volte al miglioramento del SGSI.

SEZIONE 10 – MIGLIORAMENTO

In questa fase si prevede di mantenere attivo, aggiornare e migliorare il SGSI mettendo in atto Azioni Correttive, basate sui risultati degli Audit di primo livello, sugli esiti del Riesame di direzione o su altre informazioni pertinenti, al fine di ottenere il miglioramento continuo del SGSI.

Le principali attività in cui si articola la fase di miglioramento del SGSI sono descritte nei paragrafi seguenti.

10.1 NON CONFORMITÀ E AZIONI CORRETTIVE

Vengono intraprese le azioni correttive per eliminare le cause di situazioni di “non conformità” ai requisiti del SGSI, al fine di evitarne la ripetizione. Inoltre, sono attuate azioni preventive per eliminare le cause di potenziali “non conformità” ai requisiti del SGSI.

Di particolare importanza, in questa ottica, sono le valutazioni delle misure correttive, la cui gestione è illustrata dal documento “PSG_SGSI_Gestione Non Conformità a Azione Correttive” [22].

Nell'ambito del modello del SGSI è prevista anche una specifica fase di verifica per valutare se quanto è stato pianificato a seguito degli audit di primo livello sia stato effettivamente realizzato o se devono essere intraprese ulteriori azioni correttive o di miglioramento per mitigare i rischi. In particolare, in questa fase il responsabile delle verifiche ha il compito di:

- stabilire la data delle verifiche, in accordo con i responsabili da intervistare, secondo il Piano delle Verifiche;
- eseguire la verifica;
- controllare che siano state risolte le anomalie riscontrate durante le precedenti verifiche;
- esaminare l'efficacia delle azioni correttive implementate;
- definire l'attuazione di nuove misure correttive o delle azioni di miglioramento.

Tale ruolo viene attribuito all'Ufficio SGSI Governance.

10.2 MIGLIORAMENTO CONTINUO

L'obiettivo del miglioramento dell'efficacia del SGSI viene conseguito mediante la considerazione dei seguenti elementi:

- Implementazione SGSI;
- Obiettivi della sicurezza;
- Risultati degli Audit;
- Analisi degli eventi monitorati;
- Azioni Correttive attuate;
- Riesame da parte del Vertice.

Le attività e le azioni di miglioramento sono comunicate alle Parti Interessate in funzione del livello e viene assicurato che i miglioramenti raggiungano gli obiettivi prefissati.

ALLEGATO 1 - MATRICE DI CORRELAZIONE TRA IL MANUALE SGSI DI AGENZIA DELLE ENTRATE-RISCOSSIONE E LA NORMA ISO 27001

UNI EN CEI ISO IEC 27001: 2017		Manuale SGSI	
Rif.	Titolo Capitolo/Paragrafo	Par.	Titolo Capitolo/Paragrafo
0	INTRODUZIONE		INTRODUZIONE AGENZIA DELLE ENTRATE-RISCOSSIONE IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI L'APPROCCIO PER PROCESSI
1	SCOPO E CAMPO DI APPLICAZIONE	1	SCOPO E CAMPO DI APPLICAZIONE
2	RIFERIMENTI NORMATIVI	2	RIFERIMENTI NORMATIVI
		2.1	Normativa e documenti di riferimento
		2.2	Correlazione tra manuale e requisiti della norma
3	TERMINI E DEFINIZIONI	3	TERMINI E DEFINIZIONI
		3.1	Sigle e abbreviazioni
		3.2	Termini e definizioni
4	CONTESTO DELL'ORGANIZZAZIONE	4	CONTESTO DELL'ORGANIZZAZIONE
4.1	Comprendere l'organizzazione ed il suo contesto	4.1	Comprendere l'organizzazione ed il suo contesto
4.2	Comprendere le necessità e le aspettative delle parti interessate	4.2	Esigenze ed aspettative delle parti interessate
4.3	Determinare il campo di applicazione del SGSI	1	SCOPO E CAMPO DI APPLICAZIONE

UNI EN CEI ISO IEC 27001: 2017		Manuale SGSI	
Rif.	Titolo Capitolo/Paragrafo	Par.	Titolo Capitolo/Paragrafo
4.4	Sistema di Gestione per la Sicurezza delle Informazioni	4.3	Documenti del SGSI
5	LEADERSHIP	5	LEADERSHIP
5.1	Leadership e impegno	5.1	Leadership e impegno
5.2	Politica	5.2	Politica
5.3	Ruoli, responsabilità e autorità nell'organizzazione	5.3	Ruoli, responsabilità e autorità nell'organizzazione
6	PIANIFICAZIONE	6	PIANIFICAZIONE
6.1	Azioni per affrontare rischi e opportunità	6.1	Azioni per affrontare rischi e opportunità
6.2	Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli	6.2	Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli
7	SUPPORTO	7	SUPPORTO
7.1	Risorse	7.1	Risorse
7.2	Competenza	7.2	Competenza
7.3	Consapevolezza	7.3	Consapevolezza
7.4	Comunicazione	7.4	Comunicazione
7.5	Informazioni documentate	7.5	Informazioni documentate
8	ATTIVITA' OPERATIVE	8	ATTIVITA' OPERATIVE
8.1	Pianificazione e controllo operativi	8.1	Pianificazione e controllo operativi
8.2	Valutazione del rischio relativo alla sicurezza delle informazioni	8.2	Valutazione del rischio relativo alla sicurezza delle informazioni
8.3	Trattamento del rischio relativo alla sicurezza delle informazioni	8.3	Trattamento del rischio relativo alla sicurezza delle informazioni

UNI EN CEI ISO IEC 27001: 2017		Manuale SGSI	
Rif.	Titolo Capitolo/Paragrafo	Par.	Titolo Capitolo/Paragrafo
9	VALUTAZIONE DELLE PRESTAZIONI	9	VALUTAZIONE DELLE PRESTAZIONI
9.1	Monitoraggio, misurazione, analisi e valutazione	9.1	Monitoraggio, misurazione, analisi e valutazione
9.2	Audit Interno di primo livello	9.2	Audit Interno di primo livello
9.3	Riesame di direzione	9.3	Riesame di direzione
10	MIGLIORAMENTO	10	MIGLIORAMENTO
10.1	Non conformità e azioni correttive	10.1	Non conformità e azioni correttive
10.2	Miglioramento continuo	10.2	Miglioramento continuo