delle procedure ad essa collegate **non è una prerogativa esclusiva della Direzione, ma è una precisa responsabilità di tutto il personale dipendente, dei collaboratori esterni e dei fornitori critici.**
A tal fine, Sonicatel esige l'applicazione della policy del "minimo privilegio", promuove l'etica della responsabilità (Accountability) e vincola la propria catena di fornitura al rispetto di standard equivalenti (es. Data Processing Agreement e NDA).

4.5 Impegno al Miglioramento Continuo

Sonicatel S.r.l. si impegna a migliorare continuamente l'idoneità, l'adeguatezza e l'efficacia del proprio SGI. Attraverso l'applicazione del ciclo di Deming (Plan-Do-Check-Act), l'analisi sistematica dei dati di monitoraggio (Zabbix/Cacti), la gestione rigorosa delle Non Conformità, l'analisi degli incidenti sfiorati (Near-Miss) e l'esecuzione di Audit Interni, la Direzione trasforma ogni criticità in un'opportunità di evoluzione dei propri processi.

L'azienda consente Audit di seconda parte, solo se:

- Invio formale mezzo PEC della richiesta con relative motivazione
- Pianificazione dell'Audit con almeno 15 giorni di preavviso
- Che il personale utilizzato per l'audit sottoscriva clausola di riservatezza
- Che non fuori esca o sia richiesta copia di nessun documento relativo ai sistemi IT e di sicurezza.

La politica sarà distribuita, mediante:

- Mediante posta elettronica
- Mediante bacheche presenti nei locali aziendali

La presente Politica è comunicata, compresa e applicata all'interno dell'Organizzazione. È inoltre resa disponibile alle Parti Interessate rilevanti tramite i canali di comunicazione ufficiali di Sonicatel S.r.l. (Sito Web istituzionale e documentazione contrattuale). La Direzione si impegna a riesaminarla con cadenza almeno annuale o in concomitanza di cambiamenti significativi del contesto operativo.

L'Amministratore Unico
(Angelo Torzi)

la *Threat Intelligence*, il monitoraggio continuo (sistemi Zabbix/Cacti) e l'analisi dei "Near-Miss" (incidenti sfiorati), le minacce vengono identificate e mitigate prima che possano impattare sul cliente.

B. Security & Privacy by Design e by Default
Fin dalla fase di "Sopralluogo Tecnico Integrato" e di "Progettazione Logica" per un nuovo cliente o per lo sviluppo di nuovi automatismi (software/AI), Sonicatel integra nativamente i controlli di sicurezza. L'architettura prevede di default la segregazione delle reti (VLAN dedicate), regole di firewalling stringenti, la disattivazione dei protocolli insicuri (Hardening) e la minimizzazione dei dati personali raccolti, garantendo che le configurazioni base siano sempre le più sicure.

C. Tutela della Triade RID e Classificazione degli Asset
Tutto il patrimonio informativo aziendale e dei clienti è classificato e protetto secondo le tre dimensioni fondamentali della sicurezza (ISO 27001):

- Riservatezza (Confidentiality): Garantita dall'uso di crittografia per i dati in transito (VPN, TLS) e dalla rigorosa adozione del Principio del Minimo Privilegio (Least Privilege). L'accesso ai sistemi avviene solo tramite utenze nominali, protette da caveau crittografati (KeePass) e Autenticazione a Più Fattori (MFA), in un'ottica di progressiva evoluzione verso logiche *Zero Trust*.
- Integrità (Integrity): Assicurata dall'impossibilità di alterazione dei log critici (CGNAT) e dei backup, mediante l'impiego di funzioni di hashing (SHA-256) e storage in modalità WORM (Object Locking).
- Disponibilità (Availability): Garantita attraverso la Resilienza Dinamica. La continuità non è affidata al solo salvataggio del dato, ma è progettata architetturalmente tramite ridondanza dei nodi core, failover automatici su reti indipendenti (4G/LTE) e sincronizzazione a caldo dei servizi in ecosistemi Cloud qualificati.

D. Consapevolezza ed Etica della Responsabilità (Human Firewall)
L'infrastruttura tecnologica più avanzata è inefficace senza il supporto del fattore umano. Sonicatel riconosce che ogni dipendente e collaboratore rappresenta la prima linea di difesa. Per questo, l'azienda promuove una "blame-free culture" (cultura senza colpa) volta alla segnalazione trasparente delle anomalie e investe costantemente in *Security & Privacy Awareness* per contrastare minacce come il Social Engineering e il Phishing.

E. Resilienza Climatica e Adattamento (ISO Amendment 2024)
Sonicatel riconosce il cambiamento climatico come un fattore critico capace di influenzare la propria infrastruttura (es. eventi estremi sui nodi FWA o stress termico sugli apparati). La Direzione si impegna a valutare costantemente tali rischi esogeni, integrandoli nei processi di progettazione (scelta di Data Center qualificati) e nei piani di Disaster Recovery, al fine di garantire la continuità dei servizi e la protezione degli asset anche in condizioni ambientali avverse.

4.4 Responsabilità di Osservanza e Attuazione
L'efficacia del Sistema di Gestione Integrato dipende dal fattore umano. L'osservanza di questa Politica e

- Assicurare la trasparenza e l'esattezza nelle fasi di progettazione, attivazione (delivery) e fatturazione dei servizi, mantenendo allineate le aspettative del cliente con le reali capacità dell'infrastruttura tecnologica.

B. Conformità Cogente per il Settore ISP (Requisiti Normativi e Autorizzativi)

- Operare nel rigoroso rispetto del Codice delle Comunicazioni Elettroniche (D.Lgs. 259/2003 e s.m.i.) e delle relative Delibere dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM), assicurando la trasparenza tariffaria, la qualità del servizio e la corretta gestione delle procedure di portabilità (Number Portability).
- Assicurare la tempestiva collaborazione con l'Autorità Giudiziaria per le finalità di accertamento e repressione dei reati (Lawful Interception), garantendo la massima riservatezza delle indagini.

C. Tutela della Privacy e Sicurezza (Requisiti Legali sulla Protezione dei Dati)

- Garantire la conformità assoluta al GDPR (Regolamento UE 2016/679) e al Codice Privacy (D.Lgs. 196/2003), applicando i principi di *Privacy by Design* e *by Default* in ogni nuovo processo o architettura.
- Adempiere in modo stringente all'obbligo di Data Retention (Legge 167/2017) per i dati di traffico telematico (log CGNAT e CDR), garantendone l'integrità, la conservazione sicura per 72 mesi tramite tecnologie immutabili (WORM/Object Locking) e l'inaccessibilità a personale non autorizzato.
- Rispettare le prescrizioni del Garante Privacy, con particolare riferimento al tracciamento inalterabile degli accessi degli Amministratori di Sistema (Provvedimento 17/01/2008).

D. Soddisfacimento dei Requisiti Volontari (Norme ISO e Best Practice)

- Assicurare la continua conformità dell'Organizzazione ai requisiti delle norme internazionali volontarie adottate: ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019 e ISO 22301:2019, nonché all'applicazione delle linee guida per la sicurezza in ambito Cloud (ISO/IEC 27017 e 27018).
- Rispettare le policy di sicurezza interne documentate nello *Statement of Applicability (SoA)*, imponendo l'adozione delle medesime misure di salvaguardia anche all'intera catena di fornitura (Cloud Provider e Carrier Wholesale).

4.3 Principi Generali della Gestione Integrata (Sicurezza, Qualità, Privacy e Resilienza)

In Sonicatel S.r.l., la sicurezza delle informazioni, la qualità del servizio e la continuità operativa non sono concepite come adempimenti a posteriori, ma costituiscono il DNA stesso di ogni architettura di rete e di ogni soluzione software sviluppata. La governance del Sistema Integrato si fonda sui seguenti principi cardine:

A. Approccio Basato sul Rischio (Risk-Based Thinking)

Ogni decisione strategica, tecnologica o di processo è preceduta da una rigorosa valutazione dell'impatto potenziale. Sonicatel non agisce solo in reazione ai guasti, ma adotta una postura proattiva: attraverso

- Soddisfazione e Fedeltà: Analizzare l'accuratezza amministrativa (es. correttezza della fatturazione) e monitorare il tasso di abbandono (Churn Rate) per prevenire l'insoddisfazione.

B. Obiettivi per la Sicurezza delle Informazioni (ISO/IEC 27001:2022)
Focus: Protezione della triade RID (Riservatezza, Integrità, Disponibilità) e resilienza cyber.

- Gestione Vulnerabilità: Fissare parametri stringenti per la tempestività di applicazione delle patch critiche (Vulnerability Management) sui sistemi core (es. Router MikroTik, Firewall Watchguard).
- Controllo Accessi: Raggiungere e mantenere la copertura totale dell'autenticazione a più fattori (MFA) e della segregazione delle credenziali amministrative (Identity Management).
- Integrità dei Dati: Garantire e misurare l'efficacia dei controlli crittografici (es. hashing SHA-256) applicati ai log di sistema e di traffico.

C. Obiettivi per la Protezione della Privacy - PIMS (ISO/IEC 27701:2019)
Focus: Tutela dei diritti degli interessati e compliance normativa.

- Data Retention: Garantire il rispetto assoluto delle tempistiche legali (L. 167/2017) per la conservazione dei log CGNAT e la loro successiva cancellazione sicura e automatizzata.
- Risposta agli Interessati: Misurare la tempestività nell'evasione delle richieste di esercizio dei diritti privacy (es. accesso, cancellazione) da parte di clienti e dipendenti.
- Controllo della Supply Chain: Assicurare che tutti i fornitori Cloud e Carrier Wholesale abbiano sottoscritto i relativi Data Processing Agreement (DPA) e mantengano le certificazioni richieste (es. ISO 27017/27018).

D. Obiettivi per la Continuità Operativa (ISO 22301:2019)
Focus: Resilienza delle infrastrutture e ripristino in caso di disastro.

- Continuità dell'Infrastruttura: Misurare l'Uptime reale dei nodi core e della rete di trasporto, monitorando l'efficacia degli switch automatici in caso di failover (es. passaggio su Backup 4G/LTE).
- Disaster Recovery: Pianificare e misurare l'esito delle simulazioni periodiche di ripristino, verificando il rispetto dei tempi massimi di interruzione (RTO) e della massima perdita di dati tollerabile (RPO) stabiliti nella Business Impact Analysis (BIA).

4.2 Impegno al Rispetto dei Requisiti (Compliance e Conformità)

L'Alta Direzione assume l'impegno formale, incondizionato e documentato di soddisfare tutti i requisiti applicabili all'erogazione dei propri servizi. In virtù della natura critica e fortemente regolamentata del settore delle Telecomunicazioni e dei servizi Cloud, Sonicatel declina tale impegno sulle seguenti direttrici:

A. Soddisfacimento dei Requisiti dei Clienti (Requisiti Contrattuali)

- Garantire il pieno rispetto degli impegni assunti tramite i contratti di fornitura (Business e Family), la "Carta dei Servizi" e i Service Level Agreement (SLA).

- **Test e Incident Response:** Eseguire con cadenza periodica simulazioni di ripristino (es. test mensili di restore) e mantenere piani di risposta agli incidenti cibernetici e fisici, affinché il personale sia pronto a reagire in condizioni di crisi organizzativa.

3. GOVERNANCE E MIGLIORAMENTO CONTINUO

Per assicurare che i suddetti impegni vengano sistematicamente tradotti in risultati operativi, l'Alta Direzione si impegna formalmente a:

1. **Applicazione del Risk Management:** Condurre periodiche valutazioni dei rischi (Risk Assessment Integrato), implementando Piani di Trattamento del Rischio (RTP) efficaci, basati su metodologie riconosciute a livello internazionale (es. ISO 31000).
2. **Allocazione delle Risorse:** Fornire le risorse infrastrutturali, tecnologiche e finanziarie adeguate al mantenimento e allo sviluppo del Sistema di Gestione Integrato.
3. **Sviluppo delle Competenze:** Promuovere la formazione continua e la consapevolezza (*Security & Privacy Awareness*) di tutto il personale e dei collaboratori, affinché ognuno comprenda il proprio ruolo nella prevenzione di non conformità e incidenti (es. Data Breach).
4. **Monitoraggio e Audit:** Stabilire indicatori di prestazione (KPI) sfidanti e condurre rigorosi Audit Interni integrati per verificare l'aderenza alle procedure aziendali e alle normative vigenti.
5. **Riesame della Direzione:** Valutare periodicamente l'efficacia del SGI, analizzando le deviazioni, promuovendo Azioni Correttive strutturali e spingendo l'intera organizzazione verso il **Miglioramento Continuo**.

4. PRINCIPI DI GOVERNANCE, RESPONSABILITÀ E MIGLIORAMENTO

4.1 Quadro di riferimento per gli Obiettivi del Sistema Integrato

La presente Politica Integrata costituisce il framework strategico attraverso il quale l'Alta Direzione definisce, attua e riesamina gli obiettivi per l'intero Sistema di Gestione. Per tradurre la visione aziendale in risultati operativi misurabili, la Direzione stabilisce annualmente (e documenta in un apposito *Cruscotto KPI*) obiettivi specifici, declinati sulle quattro dimensioni normative:

A. Obiettivi per la Qualità (ISO 9001:2015)
Focus: Eccellenza operativa e Customer Satisfaction.

- Erogazione del Servizio: Monitorare il rigoroso rispetto dei Service Level Agreement (SLA) contrattuali in termini di latenza, banda minima garantita (BMG) e packet loss.
- Efficienza dei Processi: Misurare e ottimizzare i tempi medi di attivazione (Time to Market) e i tempi di risoluzione dei guasti (MTTR), distinguendo tra attivazioni standard e "a progetto".

L'Organizzazione assicura l'inalterabilità di tali log mediante l'adozione di architetture storage di tipo WORM/Immutabile e procedure di *hashing* crittografico (SHA-256).

- **Gestione Vulnerabilità e Accessi:** Adottare il principio del *Least Privilege* (minimo privilegio), enforcing della *Multi-Factor Authentication (MFA)* sui sistemi critici e implementare policy stringenti per la gestione sicura degli endpoint e dei dispositivi personali (BYOD) utilizzati dal personale tecnico.
- **Conformità ai Requisiti di Sicurezza:** Assicurare l'impegno costante a soddisfare tutti i requisiti applicabili relativi alla Sicurezza delle Informazioni, derivanti dal contesto aziendale, dalle normative e dai contratti con le Parti Interessate.

2.3 Privacy Information Management System (ISO/IEC 27701:2025)

Integrando i requisiti del Regolamento (UE) 2016/679 (GDPR) all'interno dell'ISMS, Sonicatel si impegna a proteggere i Diritti e le Libertà fondamentali degli Interessati (Data Subjects), operando con trasparenza nei propri due ruoli giuridici:

- **In qualità di PII Controller (Titolare):** Per i dati di dipendenti, collaboratori e clienti diretti, l'azienda garantisce la liceità del trattamento, la limitazione della conservazione, la minimizzazione dei dati e il pieno rispetto del Registro delle Opposizioni per le attività commerciali.
- **In qualità di PII Processor (Responsabile):** Nell'erogazione di servizi Cloud (VPS, PBX, Hosting) per conto della clientela Business, Sonicatel garantisce l'isolamento logico dei *Tenant*, la cifratura dei dati in transito (es. TLS/HTTPS) e la rigida governance dei propri sub-responsabili (Sub-processors) mediante *Data Processing Agreements (DPA)* strutturati.
- **Privacy by Design:** Qualsiasi nuovo processo o architettura tecnologica viene sottoposta a valutazione preventiva (e a DPIA ove applicabile) per integrare i controlli privacy fin dalla fase di progettazione.

2.4 Continuità Operativa e Resilienza (ISO 22301:2019)

Essendo l'erogazione di connettività un servizio critico, la mitigazione dei rischi di interruzione è prioritaria. L'Organizzazione si impegna a:

- **Business Impact Analysis (BIA):** Mantenere aggiornata l'analisi degli impatti aziendali, definendo metriche rigorose per il Massimo Periodo Tollerabile di Interruzione (MTPD), l'Obiettivo di Tempo di Ripristino (RTO) e l'Obiettivo di Punto di Ripristino (RPO) per tutti i processi Core.
- **Strategie di Risoluzione (Disaster Recovery & BCP):** Progettare reti resilienti eliminando per quanto possibile i *Single Point of Failure (SPoF)*, adottando connessioni di failover per i siti critici e garantendo il backup immutabile del Sistema Gestionale e dei relativi database.

Sonicatel S.r.l. progetta ed eroga servizi di telecomunicazione (ISP), soluzioni di fonia avanzata (VoIP) e infrastrutture Cloud e di Cybersecurity (Virtual Server, PBX, Firewalling) destinate a clientela Business e Consumer. Inoltre, progetta e sviluppa sistemi software e logiche di Intelligenza Artificiale (AI) per l'automazione dei processi.
In un ecosistema digitale caratterizzato da una crescente complessità delle minacce cibernetiche, da una severa regolamentazione normativa, da una forte dipendenza dalle catene di fornitura infrastrutturali **e dai crescenti impatti sistemici derivanti dal cambiamento climatico**, la Direzione ha scelto di governare i propri processi attraverso un Sistema di Gestione Integrato (SGI) basato sull'approccio Risk-based thinking.
La presente Politica Integrata costituisce il framework strategico mediante il quale la Direzione definisce gli obiettivi aziendali, assumendosi l'impegno incondizionato di soddisfare i requisiti applicabili, soddisfare i requisiti legali e normativi cogenti e di perseguire il miglioramento continuo dell'efficacia del proprio SGI.

2. DIRETTRICI E IMPEGNI DEL SISTEMA DI GESTIONE INTEGRATO

L'Amministratore Unico stabilisce, attua e mantiene i seguenti impegni programmatici, declinati sui quattro pilastri normativi:

2.1 Gestione della Qualità (ISO 9001:2015)

L'approccio per processi adottato da Sonicatel è orientato alla massima *Customer Satisfaction* e all'eccellenza operativa. A tal fine, l'Organizzazione si impegna a:

- **Rispetto dei Service Level Agreement (SLA):** Garantire i target prestazionali definiti nella "Carta dei Servizi" in termini di latenza, *packet loss*, tempi di provisioning (TTM) e tempi di risoluzione guasti (MTTR).
- **Supply Chain Management:** Esercitare un controllo rigoroso sui fornitori strategici (Carrier di trasporto L2/L3, Upstream Provider BGP, Datacenter Cloud), misurandone oggettivamente le performance al fine di assicurare che l'infrastruttura sottostante supporti i requisiti di qualità attesi dal cliente finale.
- **Efficacia Operativa:** Standardizzare e digitalizzare i flussi di attivazione, configurazione apparati (CPE/Router) e fatturazione, riducendo l'incidenza di non conformità tecniche o amministrative.

2.2 Sicurezza delle Informazioni e Cybersecurity (ISO/IEC 27001:2022)

La salvaguardia del patrimonio informativo aziendale e dei dati affidatici dai clienti è un obbligo inderogabile. La Direzione si impegna a:

- **Protezione degli Asset (Triade RID):** Garantire la Riservatezza, l'Integrità e la Disponibilità dei sistemi, delle reti e delle informazioni, implementando i controlli organizzativi, fisici e tecnologici definiti nello *Statement of Applicability (SoA)*.
- **Conformità Legale e Data Retention:** Rispettare puntualmente le normative di settore (Codice delle Comunicazioni Elettroniche, Autorizzazione AGCOM n. 23040), garantendo la conservazione sicura dei log di traffico telematico (CGNAT e Accounting) per le finalità di giustizia.

Sede Legale ed Operativa:
Corso Gabriele Manthonè 62 – 65127 Pescara (PE)
P.IVA: 02298810694 | Numero REA: PE - 147360
Email: info@sonicatel.com | PEC: sonicatel@pec-cert.it
Web: www.sonicatel.com

POLITICA INTEGRATA DEL SISTEMA DI GESTIONE (SGI)

Conforme agli Standard Internazionali:

- **ISO 9001:2015** – Sistema di Gestione per la Qualità
- **ISO 22301:2019** – Sistema di Gestione per la Continuità Operativa
- **ISO/IEC 27001:2022** – Sistema di Gestione per la Sicurezza delle Informazioni
- **ISO/IEC 27701:2019/2025** – Privacy Information Management System (PIMS)

CONTROLLO DELLE REVISIONI

Rev.	Data	Descrizione Modifica	Redazione	Verifica	Approvazione
00	15/01/2024	Prima Emissione - Baseline SGI Integrato	SGI Mgr	C. Di Carlo	A. Torzi

RESPONSABILITÀ E APPROVAZIONE

Redazione:
Responsabile Sistema di Gestione Integrato
Firma: _____

Verifica Tecnica:
Responsabile Area Tecnica / SysAdmin (Cristhian Di Carlo)
Firma: _____

Approvazione Finale:
Amministratore Unico (Angelo Torzi)
Firma: _____

1. PREMESSA E VISIONE STRATEGICA