grifomultimedia

BETTER KNOWLEDGE
BETTER PERFORMANCE

Sicurezza delle informazioni, protezione dei dati e gestione dei servizi cloud

Applicazione integrata delle norme ISO/IEC 27001, 27017 e 27018

1. Introduzione e contesto

Grifo Multimedia S.r.l. è una realtà italiana consolidata nel panorama dei servizi digitali, specializzata in **Digital Learning, Gamification e soluzioni software innovative** per l'engagement e l'apprendimento digitale. Con oltre vent'anni di esperienza nel progettare, sviluppare e gestire piattaforme digitali, Grifo Multimedia opera in settori in rapida evoluzione e con elevate aspettative di qualità, sicurezza, affidabilità e tutela dei dati.

L'evoluzione tecnologica, l'incremento dell'adozione del cloud computing e la digitalizzazione dei processi formative e amministrativi impongono oggi una governance strutturata della sicurezza delle informazioni e dei dati personali. Questo non è solo un requisito di conformità normativa (ad esempio al GDPR), ma un elemento chiave della **fiducia nei confronti dei clienti**, della **resilienza dei servizi digitali** e della **competitività sul mercato internazionale**.

Il presente white paper esplora come l'integrazione degli standard internazionali **ISO/IEC 27001**, **ISO/IEC 27017** e **ISO/IEC 27018** possa costituire un modello di riferimento per l'adozione di un sistema di gestione completo, coerente e certificabile, specialmente per organizzazioni come Grifo Multimedia che operano nel cloud e trattano dati digitali sensibili.

2. La sicurezza delle informazioni: un imperativo per l'era digitale

La sicurezza delle informazioni non è più un concetto astratto o un insieme di tecnicismi riservati ai soli reparti IT. Per un fornitore di servizi digitali, essa rappresenta:

- la protezione degli asset informativi critici,
- la garanzia di continuità operativa anche in presenza di incidenti,
- la mitigazione di rischi reputazionali e legali,
- la capacità di rispondere a requisiti contrattuali e normativi imposti da clienti pubblici e privati.

Con l'emergere del cloud come piattaforma preferenziale di erogazione di servizi digitali e applicazioni, le organizzazioni devono affrontare rischi intrinseci legati alla **condivisione delle risorse**, alla **gestione delle identità e degli accessi**, alla **protezione dei dati personali** e alla **trasparenza operativa**.

Gli standard ISO/IEC 27001, 27017 e 27018 forniscono un quadro di riferimento consolidato a livello internazionale per affrontare questi temi con rigore, metodo e riconoscibilità.

3. ISO/IEC 27001 – Sistema di Gestione per la Sicurezza delle Informazioni

3.1 Che cos'è la ISO/IEC 27001

La ISO/IEC 27001 è lo standard internazionale che definisce i requisiti per istituire, implementare, mantenere e migliorare un **Information Security Management System (ISMS)**, un sistema di gestione documentato che permette di affrontare in modo strutturato i rischi associati alla sicurezza delle informazioni.

Questo standard non prescrive misure tecniche specifiche, ma definisce un **framework di governance** fondato su:

- una chiara comprensione del **contesto dell'organizzazione**,
- una valutazione dei rischi e la loro gestione,
- la definizione di politiche, processi e controlli coerenti con la strategia aziendale,
- un impegno permanente per il **miglioramento continuo**.

3.2 Il valore per Grifo Multimedia

Per un'azienda come Grifo Multimedia, l'adozione di un ISMS secondo ISO/IEC 27001 comporta benefici concreti:

- standardizzazione dei processi di sicurezza e delle responsabilità interne;
- riduzione sistematica del rischio di incidenti che possono compromettere servizi digitali e dati dei clienti;
- maggiore trasparenza nei confronti dei partner e delle Pubbliche Amministrazioni;
- allineamento con best practice internazionali riconosciute;
- possibilità di ottenere una **certificazione accreditata**, elemento di credibilità strategico nel mercato.

3.3 Principi chiave: un modello organizzativo solido

L'ISMS si basa su principi fondamentali:

Approccio basato sul rischio

La gestione della sicurezza non è un elenco di misure tecniche, ma un **processo decisionale basato sull'identificazione, sulla valutazione e sulla mitigazione dei rischi** che possono impattare gli asset informativi.

Leadership e governance

La direzione aziendale deve assumersi la responsabilità dell'ISMS, definire una politica di sicurezza, assegnare ruoli e responsabilità e favorire una cultura della consapevolezza nella gestione delle informazioni.

Miglioramento continuo

L'adozione di un ciclo PDCA (Plan-Do-Check-Act) consente di verificare l'efficacia del sistema, di intervenire sulle non conformità e di adattarsi a mutamenti tecnologici e di contesto.

4. ISO/IEC 27017 – Sicurezza dei servizi cloud

4.1 Perché uno standard cloud-specifico

Lo standard ISO/IEC 27017 è un'estensione della 27001 che introduce **controlli specifici per i servizi cloud**, pensati per rispondere alle peculiarità di questi ambienti:

- responsabilità condivise tra provider cloud e cliente;
- gestione multi-tenant;
- provisioning dinamico di risorse;
- dipendenza da API e servizi gestiti.

Per Grifo Multimedia, che sviluppa e gestisce soluzioni digitali e piattaforme cloud-based, questi aspetti sono centrali.

4.2 Responsabilità condivise

In un modello cloud, alcune responsabilità sono in capo al provider, altre all'organizzazione che utilizza il servizio. La ISO/IEC 27017 aiuta a:

- definire in modo chiaro le responsabilità su **gestione degli accessi**, **protezione dei dati**, **monitoraggio e logging**;
- implementare processi per la gestione delle vulnerabilità e delle configurazioni cloud;
- assicurare che la segregazione degli ambienti sia adeguata, anche in contesti multi-tenant.

4.3 Miglioramenti operativi

Con l'adozione dei controlli 27017, le organizzazioni ottengono:

- maggiore trasparenza nei servizi cloud;
- riduzione degli errori di configurazione (una delle principali cause di incidenti cloud);
- integrazione dei controlli cloud con il sistema di gestione della sicurezza globale.

5. ISO/IEC 27018 – Protezione dei dati personali nei servizi cloud

5.1 Focus sui dati personali

La ISO/IEC 27018 è la prima norma internazionale specifica per la **protezione delle informazioni personali identificabili (PII)** nei servizi cloud pubblici. Essa specifica controlli e linee guida che completano i requisiti della 27001 allineandoli ai principi di privacy e protezione dei dati.

Questo standard è particolarmente rilevante per organizzazioni come Grifo Multimedia, che trattano dati legati ad utenti, corsisti, amministratori di sistema e stakeholder delle piattaforme digitali.

5.2 Principi di trattamento dei dati personali

La ISO/IEC 27018 prescrive controlli per assicurare che:

- il trattamento dei dati personali sia lecito e trasparente;
- i dati siano raccolti per finalità esplicite, specifiche e legittime;
- la conservazione sia limitata nel tempo e proporzionata;
- siano attivate misure per garantire i diritti degli interessati (accesso, rettifica, cancellazione).

5.3 Impatti organizzativi

L'integrazione di 27018 nel sistema di gestione porta a:

- definire regole precise per la gestione dei dati personali nei servizi cloud;
- responsabilizzare i team rispetto al trattamento delle PII;
- allineare l'operatività ai requisiti del **Regolamento Europeo sulla protezione dei dati (GDPR)**.

6. Un modello integrato: 27001 + 27017 + 27018

6.1 Perché un modello integrato

L'integrazione dei tre standard consente di ottenere:

- un sistema di governance unico, coerente e scalabile;
- l'eliminazione di duplicazioni e conflitti tra controlli;
- una visione completa di rischi e controlli sia per sicurezza delle informazioni sia per protezione dei dati personali nel cloud;
- una maggiore efficienza nella gestione operativa e nella compliance normativa.

6.2 Architettura del modello

Un modello integrato comprende:

- **Policy e procedure** unificate;

- **Valutazione del rischio** congiunta per sicurezza e privacy;
- **Controlli cloud specifici** integrati nel ciclo di gestione;
- **Audit e monitoraggio** continuo su tutti gli aspetti critici;
- **Reporting e metriche** condivise.

7. Processo di implementazione consigliato

7.1 Analisi preliminare

- mappatura degli asset informativi;
- identificazione delle piattaforme digitali e dei servizi cloud in uso;
- analisi dei processi che trattano dati personali.

7.2 Valutazione e trattamento del rischio

- identificazione delle minacce e delle vulnerabilità;
- assegnazione di priorità alla mitigazione;
- definizione di piano di trattamento dei rischi e assegnazione delle responsabilità;

7.3 Definizione delle policy

- policy di sicurezza delle informazioni;
- policy di gestione cloud;
- policy di protezione dei dati personali;
- procedure operative dettagliate per implementare i controlli.

7.4 Formazione e awareness

La sicurezza è cultura: programmi di formazione dedicati a sviluppo software, operations, amministratori e utenti con ruoli di responsabilità.

7.5 Audit interno e preparazione alla certificazione

- audit di conformità interna;
- verifica dei controlli e delle evidenze;
- pianificazione della certificazione attraverso un organismo accreditato.

8. Benefici strategici e competitivi

L'adozione di un sistema integrato porta a vantaggi tangibili:

- **migliore affidabilità e resilienza** dei servizi digitali;
- **riduzione della superficie di rischio** e degli incidenti;
- **maggiore fiducia di clienti e stakeholder**;
- **posizionamento competitivo** nei mercati regolamentati;

- **coerenza operativa** con normative nazionali ed europee (GDPR).

Appendici normative e riferimenti tecnici

Appendice A – ISO/IEC 27001:2013 / 2022

- Requisiti per un ISMS;
- Allegato A: Controlli di sicurezza (A.5–A.18);
- Processi di risk assessment e risk treatment.

Appendice B – ISO/IEC 27017:2015

- Linee guida per i controlli di sicurezza dei servizi cloud;
- Responsabilità condivise provider/cliente;
- Linee guida tecniche per gestione delle identità, segregazione ambienti, logging.

Appendice C – ISO/IEC 27018:2019

- Controlli per la protezione delle informazioni personali nei servizi cloud pubblici;
- Principi di privacy by design e by default;
- Allineamento con GDPR: basi giuridiche, diritti degli interessati, criteri di conservazione.

Appendice D – GDPR (Regolamento UE 2016/679)

- Art. 5: principi in materia di trattamento dei dati personali;
- Art. 24–43: responsabilità del titolare e del responsabile del trattamento;
- Art. 32: sicurezza del trattamento;
- Diritti degli interessati (art. 15–22).

Per Grifo Multimedia S.r.l., l'adozione di un sistema integrato basato su ISO/IEC 27001, 27017 e 27018 rappresenta una **scelta strategica di governance**. Non si tratta solo di conformità, ma di costruire fiducia, affidabilità e vantaggio competitivo, specialmente in un mercato digitale globale e sempre più esigente.

Un percorso strutturato, ben documentato e orientato al miglioramento continuo consentirà all'organizzazione di consolidare la sua reputazione, proteggere i dati dei clienti e garantire servizi cloud sicuri, resilienti e trasparenti.

Bari 28/01/2026

GRIFO MULTIMEDIA S.r.l.
Presidente del Consiglio
di Amministrazione
Dott. Livio Melfi