



GM Servizi Srl
Web Marketing, Application Design & Outsourcing

via IV Novembre 71 I-18100 Imperia
phone +39 0183 660023 | fax +39 0183 661266
web www.gmserv.com | email gm@gmserv.com
c.f. | p.iva | r.i. IM 01274490083
cap. soc. 15.000 euro i.v.

GM SERVIZI AZIENDA CERTIFICATA ISO 27001:2005

GM Servizi S.r.l. è azienda certificata ISO/IEC 27001:2005 per il proprio **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI).

GM Servizi integra tale sistema al proprio Sistema di Gestione della Qualità (SGQ) certificato ISO 9001:2000, in un completo Sistema di Gestione Integrato.

Lo standard ISO/IEC 27001:2005 deriva dal precedente standard inglese BS 7799-2 ed è volto a garantire una corretta ed efficace implementazione e mantenimento del SGSI tramite la valutazione dell'impianto tecnico ed organizzativo e dei controlli che l'azienda è obbligata ad impiegare e monitorare per mantenere efficace il proprio livello di gestione della sicurezza delle informazioni.

L'impostazione di un SGSI impone di studiare a fondo la propria organizzazione aziendale, il proprio business, il mercato e le tecnologie e monitorarne le evoluzioni in modo costante.

L'ambito di operatività del SGSI di GM Servizi è rappresentato dall'insieme di attività e tecnologie utilizzate per la progettazione, sviluppo, vendita e gestione tecnica di servizi ed applicazioni internet:

LA SICUREZZA DELLE INFORMAZIONI

Sicurezza delle Informazioni significa assicurare:

- **Confidenzialità:** assicurare l'accesso alle informazioni solo agli autorizzati;
- **Integrità:** assicurare che le informazioni siano complete e non modificate;
- **Disponibilità:** assicurare che le informazioni siano accessibili agli autorizzati quando richiesto.

SGSI - SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI

La Sicurezza delle Informazioni si ottiene applicando un complesso set di controlli indicati dalla norma ISO/IEC 27001 ed impostando Politiche, Processi, Procedure, Strutture organizzative, Funzionalità hardware e software ed un costante monitoraggio per il miglioramento continuo.

Un Sistema di Gestione Sicurezza delle Informazioni ha i seguenti **obiettivi**:

- Proteggere le informazioni da accessi non autorizzati;
- Impedire che le informazioni arrivino a non autorizzati per azioni deliberate o mancanza di cura;
- Proteggere l'integrità delle informazioni salvaguardandole da modifiche non autorizzate;
- Assicurare che le informazioni siano a disposizione degli autorizzati quando ne hanno bisogno;
- Controllare l'evoluzione delle minacce e delle associate vulnerabilità;
- Mantenere i rischi a livelli accettabili attraverso l'implementazione di adeguati controlli;
- Ottemperare alle disposizioni normative e legislative inerenti la sicurezza delle informazioni;

- Assicurare la continuità delle attività aziendali;
- Mantenere tra il proprio personale un'adeguata sensibilità ai temi della sicurezza.

ANALISI DI RISCHIO

Per raggiungere questi obiettivi deve essere impostata una sistematica **Analisi e Gestione del Rischio**, che comprende:

- Identificazione dei beni (dati) aziendali rilevanti ai fini del patrimonio informativo;
- Identificazione dei rischi per tali beni attraverso una metodologia di analisi basata su:
 - Determinazione del valore dei singoli beni;
 - Identificazione delle minacce, del loro impatto sui beni e della loro probabilità di concretizzarsi;
 - Valutazione dei conseguenti livelli di rischio;
 - Definizione dei livelli di rischio residuo o accettabile.
- Riduzione ad un livello accettabile dei rischi individuati tramite l'adozione e la gestione di appositi controlli e un **Piano di Trattamento dei Rischi**;

CONTROLLI E PROCEDURE

L'Annesso A della norma ISO/IEC 27001 identifica e definisce gli obiettivi ed i controlli minimi da applicare affinché il SGSI sia certificabile secondo la norma stessa, le famiglie di controlli sono:

- **Politica della Sicurezza**
 - Definizione ambito, perimetro struttura organizzativa
 - Definizione dei Controlli e Coordinamento.
- **Organizzazione della sicurezza delle informazioni**
 - Organizzazione interna e Processi autorizzativi;
 - Accordi di riservatezza
 - Gestione Terze parti e identificazione e gestione dei rischi correlati.
- **Gestione dei Beni**
 - Inventario, classificazione e controllo dei beni e delle minacce.
- **Sicurezza delle Risorse Umane**
 - Ruoli, responsabilità e Assegnazione e rimozione diritti di accesso;
 - Selezione, condizioni di impiego, Consapevolezza, formazione e addestramento;
- **Sicurezza fisica e ambientale**
 - Definizione perimetro e aree ad accesso riservato/controllato;
 - Protezioni e Manutenzione contro minacce esterne e ambientali.
- **Gestione delle Comunicazioni e delle operazioni**

- Definizione e controllo dei sistemi di sviluppo, test e produzione;
- Procedure di Backup delle informazioni;
- Monitoraggio e controllo delle reti e dei servizi di rete;
- Controllo di malware;
- Procedure di memorizzazione e interscambio delle informazioni e Gestione dei cambiamenti.
- **Controllo degli accessi**
 - Definizione profili di autorizzazione e gestione dei privilegi e revisione dei diritti di accesso;
 - Connessioni, Protezioni e Controllo accessi di rete.
- **Acquisizione, sviluppo e manutenzione dei sistemi informativi**
 - Controllo dei processi interni e controlli nell'elaborazione nelle applicazioni;
 - Sicurezza dei file di sistema e nei processi di sviluppo e supporto;
 - Gestione e Controllo delle vulnerabilità tecniche;
 - Monitoraggio eventi e possibili minacce.
- **Gestione dei security incidents:** processi e procedure per la gestione degli eventi;
- **Business Continuity:** definizione e applicazione di piani di continuità.
- **Rispetto di Normativa e legislazione e conformità tecnica.**

GM Servizi si rende disponibile a subire un AUDIT DI VERIFICA del proprio Sistema di Gestione della Sicurezza delle Informazioni da parte dei propri clienti interessati.