CERTIFICATO

MQ-03-SSI Rev. 04

SI CERTIFICA CHE IL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI DI

GEMATICA S.R.L.

SEDE LEGALE

Via Diocleziano, 107 - 80125 Napoli (NA)

UNITA' OPERATIVA

Via Diocleziano, 107 - 80125 Napoli (NA)

E' CONFORME AI REQUISITI DELLA NORMA

ISO/IEC 27001:2022

PER LE SEGUENTI ATTIVITA'

Progettazione, installazione, messa in servizio, collaudo e manutenzione di sistemi di comunicazione su IP - Sviluppo Software.

Rif. Statement of Applicability rev. 01 del 06/04/2026

CERTIFICATO N° CE/101-SSI Rev.04

Data rilascio	Data di emissione corrente	Data di scadenza
26/05/2023	25/05/2026	25/05/2029

Il presente certificato è soggetto al rispetto del documento di Certifica S.r.l.: Regolamento di certificazione.
La validità del presente certificato è subordinata alle visite periodiche annuali e dalla verifica completa ogni tre anni del sistema di gestione per la sicurezza delle informazioni.
Per informazioni puntuali e aggiornate circa eventuali variazioni intervenute nello stato della certificazione di cui al presente certificato, si prega di contattare il n° telefonico 081/5237021 o l'indirizzo e-mail info@certificasistemi.com

IL DIRETTORE

MANAGEMENT SYSTEM CERTIFICATION
ACCREDIA
01502

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC.

Signatory of EA, IAF and ILAC Mutual Recognition Agreements.

CERTIFICA S.r.l.
Via F. Petrarca, 15 - 80070 Bacoli (NA)
Tel. 081 5237021
Partita I.V.A. 08654031213
info@certificasistemi.com
www.certificasistemi.com

Ulteriori informazioni riguardanti lo scopo del certificato e l'applicabilità dei requisiti della norma di riferimento sono disponibili su richiesta.
Il presente certificato non si riferisce alle caratteristiche di prodotto e servizi forniti dall'organizzazione certificata, si riferisce solo al sistema di gestione valutato

ORGANISMO DI CERTIFICAZIONE

La **Politica Aziendale** impone che, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali sia impostata con le regole proprie dell'applicazione del Sistema di gestione secondo la norma UNI CEI EN ISO/IEC 27001:2022.

SCOPO E OBIETTIVI

La direzione di **GEMATICA s.r.l.** ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la **Gestione della Sicurezza delle Informazioni**.

Lo scopo della presente policy è di garantire la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

CAMPO DI APPLICAZIONE

La presente Politica si applica trasversalmente a tutti i livelli e agli organi aziendali.

L'osservanza delle disposizioni in essa contenute è obbligatoria per tutto il personale. Tali prescrizioni devono inoltre essere formalmente integrate negli accordi contrattuali stipulati con qualsiasi soggetto esterno che, a qualunque titolo, sia coinvolto nel trattamento di informazioni rientranti nel campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), definito come:

"Attività IT a supporto della: Progettazione, installazione, messa in servizio, collaudo e manutenzione di sistemi di comunicazione su IP - Sviluppo Software".

La condivisione e la diffusione delle informazioni verso terzi sono rigorosamente limitate a quanto strettamente necessario per il corretto svolgimento delle attività operative e devono sempre avvenire nel pieno rispetto delle procedure interne e delle normative vigenti.

POLICY SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda. Per proteggere efficacemente questo patrimonio, è fondamentale assicurare tre requisiti chiave:

- **Confidenzialità**: le informazioni devono essere accessibili esclusivamente al personale autorizzato.

- **Integrità**: deve essere garantita la precisione e la completezza dei dati, nonché l'affidabilità dei metodi utilizzati per la loro elaborazione.
- **Disponibilità**: gli utenti autorizzati devono poter accedere alle informazioni e ai sistemi collegati tempestivamente e ogni qualvolta ne abbiano necessità.

La carenza di adeguate misure a tutela di questi principi espone l'Azienda a gravi conseguenze: danni reputazionali, insoddisfazione dei clienti, sanzioni normative e perdite finanziarie. Al contrario, un ambiente sicuro è il prerequisito fondamentale per una corretta e affidabile condivisione delle informazioni.

Per governare questi aspetti, l'Azienda si affida ad un'analisi dei rischi. Questo processo valuta le minacce potenziali, la probabilità che si verifichino e il relativo impatto sui sistemi, permettendo di definire e adottare le contromisure più efficaci.

Inoltre, tutti gli asset aziendali rilevanti sono mappati in un inventario costantemente aggiornato e affidati a un responsabile. Al fine di mantenere livelli di riservatezza e integrità coerenti e appropriati, le informazioni vengono classificate in base alla loro criticità.

Per assicurare nel concreto la protezione dei dati, l'Azienda applica i seguenti principi generali:

- Controllo degli accessi: identificazione e autenticazione obbligatorie per tutti i sistemi. Le autorizzazioni sono assegnate esclusivamente in base al ruolo (principio della necessità di conoscere) e sono soggette a revisione periodica.
- Gestione sicura degli asset: applicazione di procedure chiare e vincolanti per l'utilizzo dei beni e dei sistemi aziendali.
- Sicurezza fisica: protezione attiva degli accessi alle sedi, ai singoli locali e alle apparecchiature IT.
- Consapevolezza e Formazione: sensibilizzazione continua di dipendenti e collaboratori sui temi della sicurezza informatica, a partire dal momento dell'assunzione, e integrazione della sicurezza in tutte le fasi di progettazione e formazione ICT.
- Gestione degli incidenti: obbligo per tutto il personale di segnalare tempestivamente qualsiasi anomalia, garantendo una gestione strutturata e rapida delle emergenze.
- Continuità operativa (Business Continuity): adozione di un piano strategico per affrontare eventi imprevisti, assicurando il ripristino rapido dei servizi critici e minimizzando le conseguenze negative sul business.
- Conformità e Terze parti: pieno rispetto delle disposizioni di legge, dei regolamenti e dei vincoli contrattuali con i partner esterni, riducendo al minimo il rischio di sanzioni legali o amministrative.

RESPONSABILITÀ DI OSSERVANZA E ATTUAZIONE

L'osservanza e l'attuazione delle policy sono responsabilità di:

- Tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
- Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
- Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda, devono garantire il rispetto dei requisiti contenuti nella presente policy.

Il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni, che nell'ambito del Sistema di Gestione e attraverso norme e procedure appropriate, deve:

- condurre l'analisi dei rischi con le opportune metodologie e adottare tutte le misure per la gestione del rischio,
- stabilire tutte le norme necessarie alla conduzione sicura di tutte le attività aziendali,
- verificare le violazioni alla sicurezza e adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi,
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni,
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

RIESAME

La Direzione, supportata dal Responsabile del Sistema di Gestione (SGSI), verifica periodicamente—o in occasione di cambiamenti significativi—l'efficacia e l'efficienza del Sistema di Gestione. L'obiettivo è garantire il controllo continuo e l'adeguamento tempestivo della Politica alle evoluzioni del contesto aziendale, tecnologico e normativo.

Il processo di riesame si concentra su:

- La verifica dell'aderenza alla Politica e lo stato di avanzamento delle azioni preventive e correttive.

- L'analisi dei cambiamenti rilevanti (organizzativi, tecnici, disponibilità di risorse, vincoli legali o contrattuali) che possono impattare la sicurezza delle informazioni.
- L'esame dei risultati derivanti dai riesami precedenti.

Gli esiti del riesame devono sempre tradursi in decisioni e azioni concrete finalizzate al miglioramento continuo della sicurezza delle informazioni in azienda.

IMPEGNO DELLA DIREZIONE

La Direzione promuove attivamente la sicurezza delle informazioni attraverso direttive chiare, l'assegnazione di incarichi e l'assunzione diretta di responsabilità.

L'impegno si concretizza in azioni specifiche volte a:

- Allineare gli obiettivi: garantire che gli obiettivi di sicurezza siano definiti e coerenti con le necessità aziendali.
- Definire i ruoli: stabilire le responsabilità per lo sviluppo e il mantenimento del SGSI.
- Garantire le risorse: fornire mezzi adeguati per l'implementazione, il controllo e il miglioramento continuo del Sistema.
- Integrare i processi: assicurare che il SGSI e i relativi controlli siano parte integrante delle attività operative quotidiane.
- Promuovere l'innovazione sicura: sostenere iniziative di miglioramento e l'uso di infrastrutture IT ingegnerizzate in modo sicuro, avvalendosi anche di fornitori certificati.
- Sviluppare la cultura aziendale: attivare programmi di formazione per diffondere la consapevolezza sulla sicurezza tra tutto il personale.

Napoli, 13/04/2026

Direzione