Politica per la Sicurezza delle Informazioni

Rev. 1 del 15/04/2024

REDAZIONE/VERIFICA/APPROVAZIONE		FIRMA
Amministratore Unico	Michele P.	

SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da NeMeA Sistemi SRL al fine di sviluppare un efficace e sicuro Sistema di Gestione della Sicurezza delle Informazioni (di seguito SGSI), ed è esteso a includere la sicurezza delle informazioni gestite in ambienti cloud, in conformità agli standard ISO 27017 e ISO 27018, al fine di garantire la protezione dei dati personali e delle infrastrutture condivise.

IL CONTESTO

NeMeA Sistemi SRL è una PMI italiana leader riconosciuta nello sviluppo e implementazione di soluzioni e servizi innovativi legati alla geoinformazione, nella produzione di dati geografici, nel remote sensing RADAR. Per NeMeA la sicurezza delle informazioni è fattore irrinunciabile per la protezione del proprio patrimonio informativo e quello dei propri Clienti ed è per questo che all'interno dell'azienda viene posta particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione, sviluppo erogazione e manutenzione dei propri servizi/prodotti, ritenuti bene primario dell'azienda. Consapevole del fatto che la gestione dei servizi per i Clienti possa comportare l'affidamento di dati e informazioni critiche, NeMeA opera secondo normative di sicurezza riconosciute in ambito internazionale; NeMeA intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio la riservatezza, l'integrità e la disponibilità sia del patrimonio informativo interno che di quello che è stato ad essa affidato dai propri Clienti. Su tali basi NeMeA Sistemi SRL. ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità ai requisiti della norma internazionale UNI EN ISO/IEC 27001:2022 che tenga conto dei requisiti specifici per la gestione sicura dei dati in ambienti cloud, come previsto dalle norme ISO 27017 e ISO 27018. Tali requisiti includono la protezione contro accessi non autorizzati, la gestione delle chiavi crittografiche e il trattamento dei dati personali in conformità alle leggi applicabili

NeMeA si impegna a considerare le esigenze e le aspettative delle parti interessate (interni, clienti, fornitori e regolatori) nel definire e attuare il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

A tal fine condivide la politica per la sicurezza delle informazioni di NeMeA con tutto il personale interno, i collaboratori, i fornitori e tutte le terze parti che a vario titolo entrano in contatto con le informazioni protette dal SGSI di NeMeA .

La presente politica è distribuita mediante il sito internet aziendale, che ne mette a disposizione la versione approvata più aggiornata. Qualunque copia di questo documento non sia appena stata scaricata dal sito internet aziendale è da considerarsi non aggiornata.

Il Sistema di Gestione per la Sicurezza delle Informazioni di NeMeA definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei requisiti di sicurezza di base elencati di seguito:
- Riservatezza: l'informazione deve essere nota solo a chi dispone di opportuni privilegi;
- Integrità: l'informazione deve essere modificabile solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità: l'informazione deve essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che dispongono dei relativi privilegi. Questa politica definisce i principi di sicurezza delle informazioni che guidano:
- I comportamenti dei soggetti cui essa è indirizzata, nell'ambito del SGSI;
- L'implementazione di processi, procedure, istruzioni, l'adozione di pratiche ed altri controlli nell'ambito del SGSI. Di seguito sono espressi i principi che determinano e sostengono la definizione ed attuazione del SGSI a garanzia della sicurezza delle informazioni.

Principio 1

Il SGSI si applica a tutte le attività di analisi, progettazione, sviluppo e manutenzione di servizi e ai dati ad esse collegati, alla tutela dei prodotti e alla relativa gestione della piattaforma di media asset management NeMeA.

Principio 2

Tutte le informazioni essenziali al servizio NeMeA (ad es. documenti tecnici e commerciali, codice sorgente, informazioni di configurazione, e-mail relative al servizio, informazioni fornite dai clienti della piattaforma, ecc.) devono essere protette.

Principio 3

Tutte le informazioni da proteggere devono essere gestite secondo il livello di classificazione attribuito, nel rispetto delle relative procedure, lungo tutto il loro ciclo di vita.
Le informazioni archiviate o elaborate in ambienti cloud devono essere classificate e gestite secondo criteri specifici, definiti nelle procedure operative per il cloud, in conformità ai requisiti ISO 27017 e ISO 27018.

Principio 4

La sicurezza delle informazioni costituisce un aspetto fondamentale nel successo di NeMeA Sistemi e per il conseguimento degli obiettivi di business. Il conseguimento ed il mantenimento della certificazione ISO 27001 costituiscono una prova tangibile, visibile e valutabile da terze parti, in relazione all'impegno di NeMeA nella garanzia della sicurezza delle informazioni. La perdita o sospensione di tale certificazione è ritenuta un grave danno di immagine ed un potenziale rischio per il conseguimento degli obiettivi di business.

Principio 5

Tutti coloro i quali entrano a vario titolo in contatto con le informazioni da proteggere hanno un ruolo diretto nel successo di tale protezione. È dunque responsabilità diretta ed esplicita di tali soggetti attenersi ai principi contenuti nella presente politica ed in tutte le politiche di sicurezza applicabili ad essa correlate e garantirne il rispetto.

Principio 6

La sicurezza delle informazioni viene progettata ed attuata in modo da essere parte integrante dei normali processi e comportamenti di business, e definita in modo da non pregiudicare l'adeguatezza degli stessi ai fini ed agli scopi dell'organizzazione. La sicurezza delle informazioni in ambienti cloud è integrata nei normali processi aziendali, garantendo che le operazioni siano eseguite in conformità ai requisiti di riservatezza, integrità e disponibilità definiti per i servizi cloud.

Principio 7

Il conseguimento degli obiettivi di sicurezza viene governato mediante un approccio basato sul rischio, che prevede l'applicazione di un processo di gestione del rischio che tiene in considerazione il contesto dell'organizzazione, il campo di applicazione del SGSI, gli obiettivi dell'organizzazione.
Il processo di gestione del rischio è esteso per includere valutazioni specifiche relative ai fornitori di servizi cloud, considerando aspetti quali la sicurezza fisica e logica dei data center, la gestione degli SLA e i controlli sulla protezione dei dati personali.

Principio 8

L'organizzazione adotta un processo strutturato per la gestione degli incidenti di sicurezza delle informazioni mirato a contenerne gli impatti, ad individuarne le cause ed a favorirne la rimozione. Tutti i soggetti interessati dal SGSI sono tenuti alla segnalazione di circostanze anomale o sospette riguardo alle informazioni.
La gestione degli incidenti di sicurezza comprende specifici protocolli per i dati ospitati in ambienti cloud. Ogni violazione rilevata deve essere gestita seguendo le procedure operative previste per la mitigazione degli impatti e la notifica alle parti interessate, come previsto dalle ISO 27017 e ISO 27018

L'azienda ha dedicato personale competente per:

- Emanare tutte le norme necessarie ivi inclusa la tipologia di classificazione dei documenti affinché l'organizzazione aziendale possa condurre, in modo sicuro, le proprie attività;
- Adottare criteri e metodologie per l'analisi e la gestione del rischio;
- Suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività di NeMeA Sistemi SRL.;
- Pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale;
- Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce;
- Verificare gli incidenti di sicurezza e adottare le opportune contromisure;
- Promuovere la cultura relativa alla sicurezza delle informazioni.

Tutti i soggetti esterni che intrattengono rapporti con NeMeA devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" (NDA) all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

Gli obiettivi di sicurezza delle informazioni di NeMeA vengono definiti in relazione agli obiettivi strategici e di business ed a loro sostegno, nel rispetto degli impegni contrattuali e delle normative vigenti nelle giurisdizioni di riferimento. Il raggiungimento di tali obiettivi di sicurezza viene pianificato, attuato, monitorato e controllato con il supporto di una specifica metodologia di gestione del rischio. Gli obiettivi di sicurezza ed il grado di conseguimento degli stessi, vengono riesaminati almeno una volta l'anno, tenendo conto di specifici indicatori per il cloud, come il numero di incidenti rilevati, i tempi di risposta e la conformità contrattuale dei fornitori.

Gli obiettivi di sicurezza ed i piani per conseguirli sono definiti nel documento "Obiettivi di Sicurezza".

NeMeA Sistemi SRL verificherà periodicamente, con cadenza almeno annuale, o più frequente in caso di cambiamenti significativi per quanto concerne la sicurezza delle informazioni, l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni, e la presente politica, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento