POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DEL CLOUD

ETICA si propone sul mercato come interlocutore specializzato nell'erogazione di Servizi IT e ITC.

Il presente documento rappresenta la politica adottata da **ETICA** in materia di protezione del patrimonio informativo aziendale. Lo scopo della presente politica è quello di fornire l'indirizzo generale e strategico di **ETICA** nel breve, medio e lungo termine, per garantire la tutela e la protezione delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni degli standard della famiglia ISO 27000. L'informazione è ritenuta un asset essenziale per il business aziendale e come tale deve essere protetta. Per tale motivo è responsabilità di ogni dipendente, consulente ovvero collaboratore/terza parte di **ETICA** proteggere tutte le informazioni trattate durante le proprie attività lavorative. Il personale, interno ed esterno, deve essere consapevole dell'importanza delle informazioni trattate e, di conseguenza, agire per garantirne la protezione. Questa politica rappresenta gli obiettivi ed i requisiti generali emessi dal vertice aziendale di **ETICA** che devono essere recepiti dalle strutture aziendali, ciascuna per lo specifico ambito di competenza, affinché l'attività lavorativa sia conforme a quanto specificato nella presente politica. È compito delle funzioni aziendali preposte alla sicurezza delle informazioni tradurre tali obiettivi e requisiti in contromisure e politiche di sicurezza più specifiche, nell'ottica di ottenere un congruo Sistema di Gestione per la Sicurezza delle Informazioni.

Nel caso in cui le regole di sicurezza stabilite siano disattese da dipendenti, consulenti e/o collaboratori dell'Azienda, la Direzione **ETICA** si riserva di adottare, nel pieno rispetto dei vincoli di legge e contrattuali, le misure più opportune nei confronti dei soggetti trasgressori.
La presente politica di sicurezza delle informazioni individua gli aspetti di sicurezza da implementare all'interno dell'organizzazione al fine di supportare la missione di **ETICA** e di perseguire i seguenti obiettivi primari:

- conformità alle normative vigenti
- salvaguardia dell'immagine aziendale
- protezione del business.

Per raggiungere tali obiettivi **ETICA**, attraverso il supporto di tutte le strutture aziendali, ciascuna per la parte di propria competenza, provvederà ad istituire un sistema di governo della sicurezza delle informazioni in grado di:

- dimostrare agli stakeholders la propria capacità di fornire con regolarità prodotti/servizi sicuri, massimizzando gli obiettivi di business;
- minimizzare il rischio di perdita e/o indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua e adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- promuovere la collaborazione, comprensione e consapevolezza del SGSI da parte dei fornitori strategici;
- conformarsi ai principi e ai controlli stabiliti dalla ISO 27001, ISO 27017 e ISO 27018, o altre

norme/regolamenti che disciplinano le attività di business in cui opera l'azienda, tra i quali, in particolare, le regolamentazioni inerenti la Privacy e la sicurezza dei dati personali (GDPR).
- Promuovere il miglioramento continuo attraverso controlli sul funzionamento del sistema di gestione impostato e tramite il raggiungimento degli obiettivi prefissati.

In particolare, per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO 27017, **ETICA** si impegna ad adottare requisiti di sicurezza che prendano in considerazione i rischi derivanti dal personale interno, la gestione sicura del multi-tenancy (condivisione dell'infrastruttura), l'accesso agli asset in cloud da parte del personale dei service provider, il controllo degli accessi (in particolare degli amministratori), le comunicazioni agli stakeholders in occasione di cambiamenti dell'infrastruttura, la sicurezza dei sistemi di virtualizzazione, la protezione e l'accesso dei dati in ambiente cloud, la gestione del ciclo di vita degli account cloud, la comunicazione dei data breach e linee guida per la condivisione delle informazioni a supporto delle attività di investigazione e forensi, nonché la costante sicurezza sull'ubicazione fisica dei dati nei server in cloud.

Inoltre, l'azienda è costantemente impegnata nella protezione dei dati personali degli interessati che gestisce, con particolare riferimento a quelli dei propri clienti. Rispetto a questi ultimi l'azienda, ai sensi della ISO 27018 e della legislazione privacy vigente (GDPR), agisce come "Data Processor" ovvero come Responsabile del Trattamento, dichiarando questo status e i relativi obblighi che ne discendono nei contratti con i clienti. Tali obblighi sono riportati anche nelle nomine a responsabile.

Il contenuto del presente documento si applica a tutto il personale interno ed esterno, alle aziende partners, ai fornitori ed outsourcers ed a chiunque entra in contatto con le informazioni la cui responsabilità è a capo di **ETICA**.
In generale, il patrimonio informativo di una azienda è costituito da qualunque tipo di aggregazione di dati che hanno un valore per l'azienda, indipendentemente dalla forma e dalla tecnologia utilizzata per il loro trattamento e conservazione. L'informazione può essere fruita in forma cartacea (documenti, lettere, elenchi, etc.), elettronica (database, dischi, nastri, etc.), verbale (riunioni, conversazioni personali e telefoniche, seminari, interviste, etc.) ed è un asset essenziale per il business aziendale. La tutela delle informazioni deve avvenire in misura proporzionale alla sua importanza a livello business e consiste nel prevedere ed implementare contromisure di sicurezza adeguate alle diverse forme ed alle differenti modalità di interazione utilizzate. In particolare, il Patrimonio Informativo di **ETICA** può essere distinto in:
- Patrimonio Informativo Cliente, costituito dall'insieme delle informazioni gestite da **ETICA** attraverso i servizi forniti e attualmente localizzate nel proprio Data Center.
- Patrimonio informativo interno, costituito da tutte le informazioni interne all'azienda ed in parte gestite attraverso i Sistemi Informativi i cui servizi sono forniti anche in outsourcing.

Il primo, per i suoi contenuti e per i contratti commerciali in essere, è strettamente legato al "core business" di ETICA. La sua sicurezza deve essere garantita per contratto con i Clienti e qualsiasi incidente di sicurezza avrebbe conseguenze dirette sull'immagine e sullo sviluppo del business aziendale. Il secondo deve essere comunque tutelato in quanto, oltre a rappresentare un valore all'interno dell'azienda, ha influenza sul primo condizionando direttamente o indirettamente tutte le attività di business.
ETICA ritiene che il successo della propria politica per la sicurezza dell'informazione possa avvenire attraverso l'istituzione di un Sistema di Gestione della Sicurezza delle Informazioni coerente con le

politiche e con gli obiettivi espressi dal vertice aziendale. Il raggiungimento dei risultati deve avvenire attraverso un processo di miglioramento continuo del Sistema al quale contribuiscono tutte le parti interessate tra le quali giocano un ruolo fondamentale:

- l'AD che ha il compito di definire politica e obiettivi, ruoli e responsabilità del personale e che mette a disposizione tutte le risorse per il SGSI
- il personale che utilizza il Sistema e mette in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati
- i clienti che usufruiscono dei vari servizi e che devono essere garantiti per le loro esigenze di sicurezza, in misura conforme agli impegni assunti da
- i fornitori che contribuiscono, in quanto partner, al raggiungimento degli obiettivi dell'organizzazione, e che accettano le politiche di sicurezza ed i rischi connessi alla fornitura;

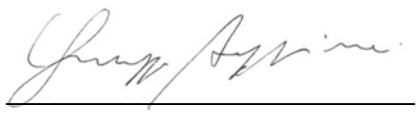
Il vertice aziendale è consapevole che la realizzazione del Sistema di Gestione richiede uno sforzo iniziale significativo e che il mantenimento e il miglioramento continuo devono essere garantiti da un supporto organizzativo adeguato. A tale scopo saranno apportate modifiche all'organizzazione di **ETICA** in modo tale che i ruoli e le responsabilità sulla Sicurezza delle Informazioni siano definiti e siano in grado di operare nella direzione indicata dalla presente politica. La Direzione renderà disponibili gli investimenti idonei a soddisfare le politiche e gli obiettivi stabiliti e ritiene opportuno affrontare la fase di avvio del Sistema con l'inserimento di risorse esterne che siano in grado di dare il loro supporto qualitativo e quantitativo su tutti gli aspetti inerenti la sicurezza delle informazioni.

La Politica per la Sicurezza delle Informazioni deve essere sempre coerente con gli obiettivi di business aziendali e pertanto la Direzione si riserva di apportare eventuali modifiche al presente documento in base al conseguimento dei risultati di **ETICA** alle aspettative di tutte le parti interessate, all'andamento del mercato di riferimento. In accordo alla Politica della Sicurezza delle Informazioni e con cadenza almeno annuale, il vertice aziendale fisserà gli obiettivi per la Sicurezza utilizzando anche i risultati raggiunti nel corso dell'anno precedente.

La politica viene regolarmente verificata al fine della sua adeguatezza in occasione del riesame della direzione, prendendo in considerazione i cambiamenti del contesto, il quadro normativo di riferimento e gli altri requisiti applicabili all'azienda.

Besana Brianza (MB), 03 Aprile 2025

L'Amministratore Delegato



(Ing. Giuseppe Azzinari)