POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La Direzione di Omniadoc S.p.A., società fornitrice di servizi e soluzioni relative alla Gestione Elettronica Documentale, crede che l'etica e la qualità della gestione organizzativa rappresentino la migliore assicurazione per il corretto funzionamento dell'azienda e costituiscano il fondamentale requisito per garantire la business continuity, migliorare costantemente la competitività sui mercati e aumentare la fidelizzazione dei clienti.
Implementando lo schema ISO 27001:2013, l'Organizzazione vuole rafforzare il suo concetto di sicurezza delle informazioni, nell'ambito dei servizi offerti, considerando come tale ogni azione di prevenzione, pianificazione, controllo e miglioramento finalizzata a ridurre l'accadimento di eventi dannosi e la gravità di questi ultimi tramite un'accorta valutazione dei rischi.

Il Codice Etico deliberato ed adottato da Omniadoc S.p.A. (di seguito "Azienda" o "Organizzazione") richiama ogni soggetto a vario titolo interessato (amministratori, dipendenti, collaboratori, fornitori,...) a tenere un comportamento conforme ai principi di onestà, lealtà, correttezza, sicurezza, professionalità, efficacia, riservatezza, trasparenza, imparzialità e responsabilità, esplicitati come segue:

- **Il rispetto delle leggi e delle norme vigenti** è principio imprescindibile per ogni soggetto che collabori con l'Azienda. In nessun caso devono essere posti in essere comportamenti che possano determinare un conflitto di interessi, corruzione e/o di fattispecie di reato di cui alla legge 231/01;
- **Si adotta il principio di Trasparenza**, fatti salvi il rispetto e la tutela della privacy, verso gli azionisti riguardo alla regolarità della gestione dell'Azienda, garantendo chiarezza nei processi decisionali nel rispetto delle responsabilità e delle competenze assegnate;
- L'Azienda rispetta i principi di **onestà, lealtà e correttezza** nei confronti dei propri clienti e del personale, presentando e proponendo unicamente servizi e/o soluzioni per le quali può garantire l'erogazione in proprio o tramite partner, sottoscrivendo regolare contratto di fornitura, applicando prezzi e tariffe congruenti con il mercato e con una corretta gestione aziendale, rifiutando qualsiasi comportamento che possa ottenerle illeciti vantaggi rispetto alla concorrenza;
- L'obiettivo di **garantire e proteggere il patrimonio aziendale**, sia tangibile che intangibile, viene perseguito:
  - ponendo costante attenzione alla **Sicurezza degli ambienti di lavoro**, valutando i rischi connessi e adottando le forme di protezione e prevenzione necessarie, sia generali che personali, soprattutto attraverso un'adeguata formazione;
  - **fornendo e mantenendo adeguati gli strumenti** tecnologici **e le conoscenze** necessarie per lo svolgimento delle attività di competenza, definite per ruolo e per mansione, sostenendo la crescita professionale;
- L'Azienda implementa e applica un **Sistema di Gestione della Sicurezza delle Informazioni**, secondo i dettami della norma ISO 27001:2013, valutando tutti i rischi connessi alla gestione delle informazioni e ponendo in atto tutte le misure atte a garantire la confidenzialità, l'integrità e la disponibilità delle stesse.
- **L'efficacia dell'organizzazione** viene perseguita attraverso il costante monitoraggio dei processi gestionali interni di qualsiasi livello, adottando le necessarie misure correttive in una prospettiva di miglioramento continuo. Questa attenzione si traduce in vantaggi competitivi riassumibili come segue:
  - maggiore economicità di gestione
  - miglioramento della soddisfazione del cliente
  - miglioramento dell'offerta di servizi e soluzioni
  - operatività secondo il principio di tutela ambientale, rispettando le normative in materia ambientale, promuovendo azioni che tutelino e preservino l'ambiente.

La politica della sicurezza delle informazioni di Omniadoc S.p.A. rappresenta l'impegno dell'Organizzazione nei confronti di Clienti e Terze Parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività e si ispira inoltre ai seguenti principi:

a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
c. Garantire che l'Organizzazione e le Terze Parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza e al mantenimento degli SLA garantiti dal SGSI.
d. Garantire che l'Organizzazione e le Terze Parti che collaborano al trattamento delle informazioni abbiano piena consapevolezza delle problematiche relative alla sicurezza.
e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
f. Garantire che l'accesso alle sedi e ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le Terze Parti.
h. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

Omniadoc S.p.A., come fornitore di servizi cloud, s'impegna nell'implementare le proprie policy al fine di mantenere costantemente adeguati i livelli di sicurezza delle proprie infrastrutture.
Nella definizione delle policy di sicurezza si terrà conto di quanto segue:

a. dei requisiti di sicurezza delle informazioni di base applicabili alla progettazione e all'implementazione del servizio cloud;
b. dei rischi da insider autorizzati;
c. dell'isolamento del cliente multi-tenancy e servizio cloud (inclusa la virtualizzazione);
d. del controllo rigoroso degli accessi alle risorse del cliente al servizio cloud;
e. del costante incremento della sicurezza nel controllo degli accessi;
f. della comunicazione ai clienti del servizio cloud durante la gestione del cambiamento;
g. della sicurezza della virtualizzazione;
h. dell'accesso e protezione dei dati dei clienti del servizio cloud;
i. della gestione del ciclo di vita degli account dei clienti del servizio cloud;
j. della comunicazione delle violazioni e linee guida per la condivisione delle informazioni a supporto di indagini generali e indagini forensi.

Gli impegni sopra esposti, oltre ad essere diffusi e monitorati continuamente, sono periodicamente consuntivati alla Direzione, al fine di avere costantemente il quadro dell'andamento degli impegni e delle attività.

Pasian di Prato, lì 11 Giugno 2024

Omniadoc S.p.A
L'Amministratore Delegato
Andrea Corson