# Politica del Cloud

**ATTENZIONE**
Il presente documento è disponibile in copia originale nella rete aziendale.
Ogni copia cartacea si ritiene copia di lavoro non controllata.
È responsabilità di chi utilizza copie non controllate verificarne il livello di aggiornamento.

| Versione | Data | Oggetto (Sintetica descrizione dei cambiamenti) | Redatto | Verificato | Approvato |
|---|---|---|---|---|---|
| **01** | 30/12/2021 | Prima emissione | RSGI | RSGI | RP |
| | | | | | |
| | | | | | |
| | | | | | |

Nome file: *POL 02 - Politica del Clod.docx*

## SOMMARIO

# 1 Scopo e campo di applicazione

Lo scopo del presente documento è quello di descrivere i principi generali definiti da TECSIS Srl al fine di erogare servizi in modalità Cloud.

La politica del Cloud si applica a tutto il personale interno, alle terze parti che collaborano alla erogazione dei servizi ed a tutti i processi e risorse coinvolte nella mission della struttura organizzativa nonché di tutti gli utilizzatori dei servizi proposti.

La presente politica è diffusa a tutti i soggetti sia interni che esterni interessati nonché sarà oggetto di riesame annuale.

# 2 Politica del Cloud

TECSIS Srl opera da protagonista nel mercato dell'Information Technology & Communication con la proposta e fornitura di soluzioni software gestionali, consulenza e servizi di System Integration.

Le competenze espresse da TECSIS Srl derivano da anni di esperienza in progetti privati e pubblici con particolare indirizzo agli ordini professionali.

Gli obiettivi etici principali di TECSIS Srl sono:

- avere, sempre, un rapporto di correttezza nei riguardi dei clienti e dei fornitori che sono entrambi visti come partner strategici;
- creare un'azienda in cui l'aggiornamento tecnologico sia tale da evitare l'obsolescenza culturale e con l'ambizione di utilizzare sempre le tecnologie più avanzate che il mercato informatico è in grado di mettere a disposizione.

In tale ottica riconoscendo l'importanza strategica delle risorse umane, dei dispositivi informatici, delle infrastrutture e del patrimonio delle informazioni, TECSIS Srl ha deciso di tutelarne la salvaguardia in tutte le fasi dei processi aziendali considerando l'Information Security uno strumento che permette la condivisione sicura delle informazioni, il miglioramento delle prestazioni rese ai Clienti e della propria immagine.

Obiettivi di TECSIS Srl sono quindi:

- certificazione del Sistema di Gestione Integrato per la Qualità e per la Sicurezza delle Informazioni con estensione ai controlli ISO/IEC 27017 e ISO/IEC 27018 e mantenimento del Sistema di Gestione Integrato nel triennio successivo;
- rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il rischio residuo a livelli accettabili;
- definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (Business Continuity);

- riduzione delle vulnerabilità dei propri asset aziendali da minacce quali virus, software nocivo ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:
  - sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
  - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
  - servizi (posta elettronica e accessi al portale).
- caratterizzazione della propria offerta di servizi ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in TECSIS Srl e/o definite in sede contrattuale.

TECSIS Srl al fine di proteggere le informazioni dei Clienti archiviate e gestite in Cloud, in conformità dello standard ISO/IEC 27017:2015, considera:

- le informazioni archiviate nell'ambiente del Cloud cui il Cliente può avere accesso e che sono gestite dal Provider del Cloud (CSP);
- gli asset mantenuti sul Cloud, come le applicazioni;
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale;
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud dei Clienti che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente).
- I requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- I rischi derivanti da addetti ai lavori autorizzati;
- accesso agli asset del Cliente da parte del Provider
- procedure per il controllo accessi;
- comunicazioni con il Cliente durante il change management;
- allineamento e sicurezza degli ambienti virtuale e cloud;
- accesso ai dati del Cliente del servizio Cloud e loro protezione;
- gestione del ciclo di vita dell'account del Cliente;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni.

TECSIS Srl mette in pratica una Privacy Policy descrivendo le modalità con cui tratta i dati personali nell'ambito della erogazione del servizio di Cloud Computing, anche alla luce degli obblighi imposti dal Regolamento UE 2016/679.

TECSIS Srl in qualità di Service Cloud Provider assicura che vengano soddisfatte le seguenti condizioni:

- I dati archiviati sui server rimangono sempre di proprietà del Cliente;
- Impone adeguati controlli di accesso e garantisce che i dati in transito e il caricamento o il trasferimento di file siano protetti con protocolli di crittografia;
- Concede al cliente la possibilità di scaricare una copia dei dati di cui il cliente stesso è titolare in qualsiasi momento durante la vigenza del contratto ed in totale autonomia e dichiara con la massima trasparenza il luogo fisico dove risiedono i dati;
- Fornisce al cliente di poter monitorare periodicamente la sua risposta alle prestazioni e al rispetto del contratto.

In tale ambito, il percorso definito dalla Direzione prevede:

- Certificazione del Sistema di Gestione della Sicurezza delle Informazioni con estensione ai controlli ISO/IEC 27017 e ISO/IEC 27018 e mantenimento della stessa nel triennio successivo;
- Rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il rischio residuo a livelli accettabili;
- Attuazione, ove necessario, di idonee azioni correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
- Definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (business continuity);
- Stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

Relativamente allo Standard ISO/IEC 27018 TECSIS Srl garantisce l'implementazione dei controlli richiesti per il trattamento di dati personali implementando adeguate misure di protezione, nel rispetto dei seguenti requisiti:

Scelta e Consenso: agevolazione dell'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'interessato, attraverso le indicazioni specificate nel contratto.

Finalità del trattamento: le finalità del trattamento sono rese note nel contratto di servizio.

Minimizzazione dei dati: file e documenti temporanei sono cancellati o distrutti entro un periodo specificato e documentato.

Limitazione all'uso, alla conservazione e alla divulgazione: Non avviene la divulgazione di dati personali a terze parti. La richiesta di divulgazione di dati personali da parte di autorità amministrative o giudiziarie è notificata al cliente in maniera tempestiva, ove consentito dalla legge.

Trasparenza: il ricorso a subappaltatori da parte del provider è reso noto al cliente del servizio Cloud prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto tra il provider e il cliente. Il provider informa il cliente in modo tempestivo di eventuali modifiche previste in questo senso.

Accountability: In caso di violazioni che comportano perdite, diffusione o modifica dei dati personali (data breach), effettua la notifica tempestivamente al cliente attraverso un processo interno di Incident Management.

Conformità alla privacy: il provider indica i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e indica specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Il provider informa tempestivamente il cliente di eventuali modifiche previste a tale riguardo.

Inoltre, le seguenti azioni sono assicurate nel senso più esteso dei controlli Cloud:

- Fornisce procedure di accesso sicuro per qualsiasi account richiesto dal Cliente del servizio Cloud per gli utenti sotto il suo controllo;
- Fornisce le informazioni al Cliente del servizio Cloud in merito alle circostanze in cui utilizza la crittografia per proteggere le informazioni personali che elabora;
- Effettua smaltimento sicuro o riutilizzo, delle apparecchiature contenenti supporti di memorizzazione;

- Effettua la valutazione del rischio e attua misure tecniche e organizzative per ridurre al minimo i rischi identificati. Accordi di riservatezza o di non divulgazione tra il provider e i suoi dipendenti e collaboratori;
- Implementa meccanismi per il backup off-site per la protezione dalla perdita di dati, garantendo continuità alle operazioni di trattamento dei dati e fornendo la possibilità di ripristinare le operazioni di trattamento dei dati dopo un evento dirompente;
- Limitazione della creazione di materiale cartaceo (comprese le stampe che contengono dati personali);
- Procedure di controllo e registrazione del ripristino dei dati;
- Procedura di autorizzazione per i dati personali trasferiti su supporti magnetici al di fuori dei locali aziendali del provider e crittografia dei contenuti;
- Divieto di utilizzo di supporti e dispositivi di memorizzazione portatili non crittografati a meno di eccezioni;
- Crittografia dei dati che vengono trasmessi sulle reti pubbliche;
- Smaltimento sicuro dei materiali cartacei;
- Utilizzo di ID univoci per i clienti cloud;
- Stesura e aggiornamento sistematico di un registro degli utenti che accedono al sistema e dei relativi profili di accesso;
- Gestione degli ID utente e divieto di assegnazione ad altri di quelli non utilizzati o scaduti;
- Evidenza dei controlli minimi di sicurezza nei contratti con clienti e subappaltatori;
- Garanzia che ogni volta che lo spazio di archiviazione dei dati viene assegnato a un servizio Cloud, tutti i dati che precedentemente risiedevano su tale spazio di archiviazione siano stati resi intellegibili;
- Raggiungere la conformità rispetto alle condizioni contrattuali concordate con il Provider del Cloud pubblico che tratta Informazioni Personali Identificabili e con i Clienti del servizio Cloud.

Il Sistema di Gestione identifica e tiene conto dei requisiti derivanti dall'evoluzione del contesto interno e del contesto esterno, in particolare dei requisiti delle terze parti interessate, e identifica gli obiettivi di sicurezza da perseguire. L'Alta Direzione si impegna ad allocare le risorse necessarie alla realizzazione del predetto sistema e mantiene un "commitment" adeguato sulle tematiche della sicurezza, assicurando che gli obiettivi di sicurezza siano integrati nei processi aziendali e conseguiti.

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, tutto lo Staff di TECSIS Srl si impegna a prestare la propria disponibilità e collaborazione nell'attuazione ed aggiornamento del Sistema e ad attenersi scrupolosamente alle prescrizioni contenute nella documentazione del Sistema di gestione nel quale è previsto il Sistema per la Sicurezza delle Informazioni, nelle Procedure Operative e nelle altre disposizioni in merito predisposte dal management.