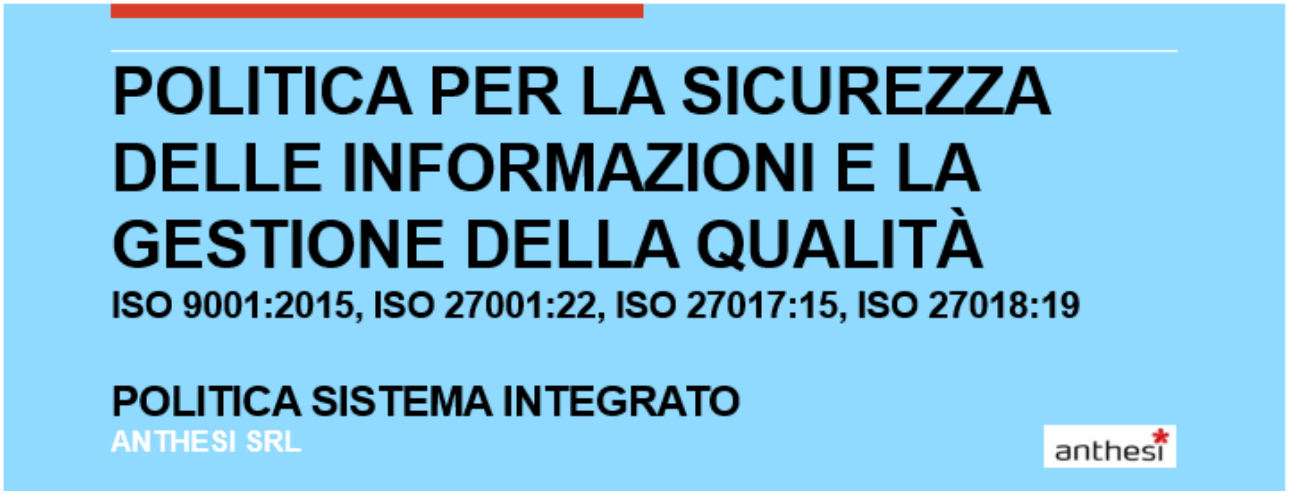

La società Anthesi srl ha l'obiettivo di affiancare le organizzazioni pubbliche e private nel processo di innovazione, modernizzazione ed orientamento dei servizi ad Internet, ricercando ed ottenendo la semplificazione e l'incremento dell'efficienza anche per i processi più complessi.

Classificazione di sicurezza	Pubblico
Versione	7
Data	2/05/2024
Approvazione	DIR

Anthesi srl

Anthesi srl opera in qualità di Cloud Service Provider nei confronti dei propri clienti per offrire servizi in cloud computing in modalità SaaS. Per l'erogazione di detti servizi si avvale di propri fornitori nei confronti dei quali assume il ruolo di Cloud Service Customer. Con riferimento ai propri clienti Anthesi srl, ai sensi della ISO/IEC 27018 e in accordo con Regolamento (UE) 2016/679, agisce come Titolare ovvero come Responsabile del Trattamento, dichiarando il rispettivo status e i relativi obblighi che ne discendono nei contratti sottoscritti e nelle nomine a responsabile che Anthesi srl prevede con i propri fornitori per lo svolgimento delle attività di trattamento. Anthesi è iscritta nel Portale META della P.A.

La sicurezza delle informazioni, la tutela dei dati personali, la qualità dei servizi IT e la continuità operativa costituiscono un processo sia tecnologico che organizzativo; di conseguenza l'organizzazione ha predisposto una serie di procedure operative standard unitamente ad attività formativa rivolta al proprio personale addetto. Le politiche di sicurezza, le procedure operative e la valutazione dei rischi sono riviste ed eventualmente aggiornate con periodicità almeno annuale, al fine di recepire nuovi indirizzi di business, evoluzioni tecnologiche e normative pertinenti.

A garanzia delle proprie attività Anthesi srl ha implementato il:
SISTEMA DI GESTIONE DI SICUREZZA DELLE INFORMAZIONI, in conformità alla Norma UNI CEI EN ISO/IEC 27001:2022, e alle linee guida ISO/IEC 27017 e ISO/IEC 27018
SISTEMA DI GESTIONE DELLA QUALITÀ in conformità alla ISO 9001:2015.
REGOLAMENTO GENERALE EUROPEO PROTEZIONE dei dati personali GDPR 2016/679

Anthesi si impegna nella protezione dei dati forniti dai committenti che vengono acquisiti durante le relazioni di natura commerciale e di natura tecnica attraverso il continuo miglioramento dei controlli della sicurezza e delle misure di tutela dei dati personali e non, al fine di proteggere la **riservatezza, l'integrità e la disponibilità** delle risorse informatiche e dei relativi sistemi di informazione.

A tal fine assicura di:

1) **rispettare** le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere, conformandosi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera la Anthesi srl, tra i quali, in particolare le regolamentazioni inerenti i trattamenti dei dati personali e la loro sicurezza.
2) **dimostrare** agli stakeholders la propria capacità di fornire con regolarità servizi informatici sicuri, massimizzando gli obiettivi di sicurezza, anche promuovere la collaborazione, comprensione e consapevolezza da parte dei fornitori strategici;
3) **minimizzare** il rischio di perdita e/o indisponibilità dei dati gestiti, pianificando e gestendo

le attività a garanzia della continuità di servizio, svolgendo una continua ed adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema, controllando con continuità il corretto funzionamento degli asset aziendali al fine di rilevare eventi anomali, incidenti e vulnerabilità dei sistemi informativi per rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;

4) **migliorare** con continuità il sistema di sicurezza delle informazioni al fine di rendere sempre più efficiente e sicuro il sistema informativo.

Campo di applicazione

"Progettazione ed erogazione di servizi di digitalizzazione online dei processi gestionali/amministrativi anche attraverso l'implementazione e la manutenzione di sistemi informativi definiti su specifiche del cliente. Erogazione di servizi SAAS con utilizzo di tecnologia cloud"

Politica

La politica si applica a tutta l'organizzazione intesa come processi, persone, strutture, strumenti, pratiche operative e sistemi di gestione ed ha come obiettivo primario:

la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, e la loro gestione, per definire e mantenere un sistema di gestione sicura delle informazioni;

l'implementazione di un sistema di gestione dei processi improntato alla soddisfazione dei clienti e al miglioramento continuo dei processi.

Questo significa, a tal fine ha sviluppato una politica che:

• sia **appropriata alle finalità e al contesto** dell'organizzazione e supporta i suoi obiettivi strategici;

• costituisca un **quadro di riferimento** per fissare gli obiettivi di tutti i sistemi di gestione applicabili, che sono sviluppati in coerenza con i principi generali e specifici e alle azioni indicate in questo documento;

• comprenda un **impegno a soddisfare i requisiti applicabili** di tutti i sistemi di gestione, inclusi quelli cogenti e contrattuali, e a **migliorare** in modo continuo i **sistemi di gestione e** la loro **efficacia**;

• comprenda l'impegno ad essere **conforme con le leggi nazionali**, le altre leggi applicabili e gli altri requisiti sottoscritti;

• sia **disponibile** come informazione documentata alle parti interessate rilevanti;

• sia **comunicata, compresa e applicata** all'interno dell'organizzazione;

• sia **riesaminata** periodicamente per accertarne la continua idoneità,

sia diffusa a tuti gli stakeholder interni ed esterni: dipendenti, consulenti, fornitori

Il documento è classificato pubblico.

Impegni

L'organizzazione è impegnata nel mantenere e sviluppare:

- **il sistema di gestione della sicurezza delle informazioni in conformità alla ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018,**
- **il sistema di gestione dei dati personali in conformità al GDPR:2015. 2016/679,**
- **il sistema di gestione della qualità in conformità alla ISO 9001.**

A tale scopo si impegna ad adeguare ed a migliorare continuamente il Sistema di Gestione per la sicurezza delle informazioni e della qualità ed a sensibilizzare e formare gli stakeholders in merito alla sua corretta applicazione.
La Direzione deve rivedere il SGSI almeno una volta all'anno o ogni volta che si verifichi un cambiamento significativo.

Impegni nei confronti dei collaboratori e del personale

Sviluppare **programmi di sensibilizzazione per g**arantire una adeguata consapevolezza e coinvolgimento del personale nei confronti del sistema di gestione aziendale della sicurezza delle informazioni e della qualità;

Gestire una **accurata gestione del personale** consentendogli di crescere professionalmente e di sentirsi parte attiva dell'impresa, assicurando opportuni e puntuali percorsi formativi con attività di **formazione continua** in materia di sicurezza delle informazioni e della qualità;

Identificazione chiara e trasparente dei ruoli aziendali, in termini di compiti, responsabilità, attività di controllo e verifica, con organigramma aziendale, profili professionali e mansionari conosciuti e condivisi.

Impegni nei confronti dei clienti dell'organizzazione

L'accesso sicuro alle informazioni, fornendo **servizi cloud,** su piattaforme affidabili, con prestazioni verificate e continuamente monitorate, garantendo fin dalla progettazione un debito isolamento dei dati di ogni cliente tramite una puntuale compartimentazione.

Utilizzo di **backup ridondante** su diverse piattaforme di archiviazione allocate geograficamente in siti diversi per garantire nei confronti di eventuali calamità naturali e/o attacchi hacker.

Garantire **disponibilità immediata di risorse** informatiche suppletive in caso di necessità non previste, sia in termini di risorse tecnologiche, con disponibilità di server non utilizzati, sia in termini di risorse umane con qualificati collaboratori esterni selezionati.

Rispetto dei requisiti normativi e contrattuali previsti per l'erogazione dei servizi IT o che regolino specifici requisiti di sicurezza delle informazioni, nonché il rispetto degli impegni di sicurezza stabiliti nei contratti con terze parti.

Implementare, attuare e **migliorare continuamente il Sistema di Gestione Qualità** SGQ e del sistema di gestione della sicurezza delle informazioni, che abbia come fondamento la gestione per processi e punti prioritariamente alla piena soddisfazione del cliente ed al miglioramento dell'efficienza ed efficacia dei risultati.

Assicurazione al cliente delle attività di assistenza, garantendo l'intervento **entro le 24 ore** dalla chiamata.

Assicurare miglioramento continuo delle prestazioni tecniche, con l'impegno di rilasciare almeno una **nuova release mensile.**

Impegni nei confronti dei fornitori

I fornitori vengono informati della politica di Anthesi nei confronti della sicurezza delle informazioni. Anthesi si accerta che tutti i fornitori abbiano consapevolezza dei problemi della sicurezza delle informazioni e rispettino la politica adottata dall'azienda, allo scopo di fare affidamento su fornitori qualificati e sicuri.

Scegliere fornitori che conoscano bene le minacce informatiche e siano in grado di affrontarle con tempestività, proteggendo le informazioni e garantendo continuità operativa in ogni situazione e che siano attenti alla qualità del servizio e alla sicurezza delle informazioni.

Fornitori qualificati in relazione alle prestazioni erogate, con qualifica rinnovata con periodicità annuale, registrata in occasione del riesame della direzione.

Impegni nei confronti delle generazioni future

Mettere in atto azioni per ridurre l'impatto sul cambiamento climatico causato dalle attività svolte attraverso il monitoraggio di attività al fine di renderle meno impattanti (email contro consumo di carta, riduzione di email contro produzione di CO2).

Acquisizioni di crediti di carbonio al fine di mantenere Anthesi sempre a zero emissioni nette. In questo modo Anthesi continuerà a supportare progetti di sostenibilità (es. forestazione, preservazione di foreste, etc.) rimanendo carbon neutral.