GRUPPO ZENIT

Politiche generali per la qualità, la sicurezza delle informazioni e la continuità operativa

Gruppo Zenit S.r.l. è un Managed Service Provider: eroga servizi IT in modalità gestita su infrastrutture Private Cloud in modalità IaaS, PaaS, SaaS; garantisce monitoraggio H24, SPOC H24, Incident e Problem Management. Inoltre, mette al servizio la propria esperienza trentennale nel campo della consulenza IT per la Digital Transformation e per il Change Management.

La Direzione di Gruppo Zenit ha predisposto una Politica della Qualità, della Sicurezza e della Continuità operativa attraverso la quale erogare i servizi sopra descritti garantendo qualità, sicurezza delle informazioni e continuità operativa. La direzione strategica, i principi, le regole di base e gli obiettivi di tale Politica sono stati definiti al fine di raggiungere quattro obiettivi primari:

1. Conseguire la soddisfazione del Cliente;
2. Garantire la protezione del proprio patrimonio informativo e di risorse umane, riducendo al minimo il rischio di danni provocati da incidenti di sicurezza deliberati o involontari dall'interno, dall'esterno o da potenziali minacce;
3. Garantire la resilienza e la continuità operativa dei servizi offerti così come la protezione delle infrastrutture di Gruppo Zenit;
4. Perseguire obiettivi di miglioramento continuo.

Inoltre, attraverso l'applicazione della presente politica, Gruppo Zenit intende conformarsi ai principi e ai controlli stabiliti dalla ISO 9001, 27001, 27017, 27018 e 22301 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).

La responsabilità nell'applicazione della presente Politica riguarda l'intera organizzazione aziendale, dalla Direzione fino a ogni singolo dipendente. Tale applicazione avviene nel rispetto delle leggi e delle disposizioni vigenti, dei requisiti contrattuali, delle norme e delle procedure aziendali.

Soddisfazione del cliente

La soddisfazione del cliente si pone alla base delle strategie individuate in quanto fondamentale al consolidamento della reputazione dell'azienda e della propria brand identity. La soddisfazione del cliente viene garantita mediante:

1. Erogazione di servizi e fornitura di prodotti di qualità che soddisfino i bisogni e le attese, iniziali e successive, dei clienti, in relazione al prezzo convenuto e in posizione fortemente competitiva rispetto alla migliore e leale concorrenza.
2. Tali servizi e prodotti vengono erogati nel rispetto della puntualità, del controllo dei costi, della continuità nell'erogazione, conformità a leggi e regolamenti, applicazione di best practices e standard, continuo aggiornamento e documentazione del cliente. Dimostrando agli stakeholders la propria capacità di fornire con regolarità prodotti/servizi sicuri, massimizzando gli obiettivi di business.
3. A sostegno di un servizio di qualità, Gruppo Zenit interpreta e affronta i progetti in forma di processi standardizzati. Questo approccio garantisce ottimizzazione delle prestazioni, maggiore controllo sull'andamento del progetto e sulle risorse necessarie

al raggiungimento degli obiettivi, consente di stabilire obiettivi, ruoli e responsabilità a monte oltre che calcolare e prevedere possibili rischi e le relative soluzioni di mitigazione.

Protezione del patrimonio informativo

La protezione del patrimonio informativo di Gruppo Zenit e dei propri clienti è posta al centro delle strategie conservative, di tutela e di protezione ponendo riservatezza, integrità e disponibilità al centro di tali strategie, predisponendo investimenti atti a garantire sicurezza e protezione del sistema informativo, riducendo il rischio di incidenti, minimizzando il rischio di perdita e/o indisponibilità dei dati dei clienti, pianificando e gestendo le attività a garanzia della continuità di servizio. Tali obiettivi di sicurezza e protezione vengono perseguiti attraverso:

1. Identificazione dei rischi, attraverso una continua e adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema, al fine di comprendere le vulnerabilità e le possibili minacce presenti in azienda che possono esporre a rischi di mancato raggiungimento degli obiettivi.
2. Gestione del rischio ad un livello accettabile attraverso la progettazione, attuazione, e mantenimento di idonee contromisure per la sicurezza delle informazioni, per garantire la qualità dei prodotti e servizi forniti e per la salute e sicurezza dei luoghi di lavoro.
3. Adozione dei requisiti di sicurezza, in particolare per l'implementazione ed erogazione dei servizi in cloud, ai sensi della ISO 27017. Gruppo Zenit si impegna ad adottare tali requisiti prendendo 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.
4. Tutela della confidenzialità delle informazioni assicurando che le informazioni siano:
    a. accessibili solo a chi ne è autorizzato;
    b. precise e complete;
    c. disponibili a chi ne ha i diritti di accesso.
5. Azioni tempestive ed efficaci di fronte a necessità emergenti nel corso delle attività lavorative.
6. Identificazione dei pericoli e dei rischi presenti all'interno dell'organizzazione.

Inoltre, Gruppo Zenit, nelle proprie strategie di salvaguardia del patrimonio informativo riserva la massima attenzione alla protezione dei dati personali. I dati che vengono affidati a Gruppo Zenit da clienti, fornitori, dipendenti e collaboratori vengono gestiti nel rispetto delle leggi e delle normative applicabili alla protezione dei dati e sempre in un'ottica di continuo aggiornamento secondo le *best practices* in materia di nuove tecnologie. L'impegno di Gruppo Zenit per la protezione dei dati personali si basa su principi di: trasparenza e chiarezza; base giuridica; minimizzazione dei dati; sicurezza dei dati; diritti dell'interessato; formazione e sensibilizzazione; conservazione limitata dei dati; test di

vulnerabilità e penetrazioni; audit esterni; garanzie ai clienti e fornitori. In particolare, rispetto ai propri clienti, 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.

La Direzione ed i responsabili di ogni dipartimento si impegnano affinché i principi sopra delineati vengano effettivamente ed efficacemente applicati ad ogni passaggio del processo produttivo e nei servizi che Gruppo Zenit offre ai propri Clienti, nonché nei riguardi dei propri Fornitori e del proprio personale.

Continuità operativa

La continuità operativa e la resilienza dei servizi offerti e la protezione delle infrastrutture di Gruppo Zenit sono garantite dall'attenta gestione e aggiornamento del Sistema di Gestione per la Continuità operativa (SGCO). L'impegno per la Business Continuity nasce dalla presa di coscienza della criticità dell'ambiente tecnologico in cui si inseriscono le principali attività di business. In particolare, in qualità di System Support e System Integrator su infrastrutture private cloud, le interruzioni delle operazioni possono avere impatti significativi sulle attività dei clienti: in caso di emergenze o disastri, i nostri clienti possano contare su una ripresa tempestiva e sicura dei loro servizi.

La continuità dei servizi che Gruppo Zenit offre non è solo una priorità tecnica, ma un valore centrale dell'azienda. L'infrastruttura di Gruppo Zenit si fonda su due Data Center progettati sulla base dei principali standard di Disaster Recovery, per garantire elevati standard di disponibilità e sicurezza. Il SGCO di Gruppo Zenit si basa sui seguenti principi guida:

1. Proattività nella gestione del rischio: identificare e valutare regolarmente i rischi che potrebbero influire sulla capacità di fornire servizi critici, implementando misure preventive adeguate;
2. Ripristino tempestivo e sicuro: garantire tempi di ripristino ottimali (RTO e RPO) che soddisfino le esigenze dei clienti, utilizzando le migliori tecnologie di Disaster Recovery;
3. Test e miglioramento continuo: effettuare test regolari dei piani di continuità operativa per verificarne l'efficacia, apportando miglioramenti in base ai risultati e all'evoluzione del contesto tecnologico e delle minacce;
4. Comunicazione trasparente: in caso di eventi critici, mantenere una comunicazione aperta e trasparente con i clienti e stakeholder, garantendo aggiornamenti tempestivi e pertinenti.

Rispettare la presente politica per la Continuità operativa significa:

1. Soddisfare le aspettative e la fiducia dei Clienti: il SGCO è progettato per prevenire e mitigare i possibili rischi a cui i Clienti possono essere esposti, permettendo loro allo stesso tempo di dedicarsi alle attività core business demandando a Gruppo Zenit la manutenzione e la disponibilità dei loro sistemi;
2. Proteggere le infrastrutture critiche: grazie alle aggiornate pratiche di Disaster Recovery è possibile proteggere asset critici e garantire il ripristino rapido delle operazioni in caso di interruzioni;

3. Mitigare i rischi: affrontare eventi inattesi o interruzioni non pianificate, che possono derivare da attacchi informatici, disastri naturali o guasti tecnici, attraverso un processo continuo di valutazione e mitigazione del rischio.

Miglioramento continuo

Il miglioramento continuo del Sistema di Gruppo Zenit si basa sul coinvolgimento, sulla cooperazione e la collaborazione tra le risorse aziendali. Tale obiettivo primario viene perseguito mediante:

1. Riesame periodico della Politica, degli Obiettivi e dell'attuazione del Sistema.
2. Una visione per processi che tiene in considerazione il contesto organizzativo e le strategie direzionali, la pianificazione degli obiettivi, la gestione delle risorse, degli asset, delle politiche e delle procedure, i criteri per l'autovalutazione e la verifica interna dell'organizzazione e gli stimoli verso tale miglioramento.
3. Attenzione all'ambiente circostante, affidandosi a un approccio di tipo preventivo di fronte ai problemi anziché sul controllo a posteriori e sulla relativa correzione, in modo da ridurre significativamente la probabilità di accadimento di incidenti, infortuni o altre non conformità.
4. Formazione e aggiornamento del personale, mantenendo alti livelli di performance, capacità di rispondere ai cambiamenti e individuare nuove opportunità di crescita.
5. Coinvolgimento del personale, accogliendone i contributi e le segnalazioni, in un ambiente lavorativo aperto a una comunicazione costruttiva e aperta al dialogo.
6. Promozione della collaborazione, comprensione e consapevolezza del Sistema da parte dei fornitori strategici.

La presente politica viene formulata e riesaminata dalla Direzione Aziendale. Tutto il personale, in base alle proprie conoscenze, ha la responsabilità di riferire al responsabile del Sistema qualsiasi punto debole individuato, nei sistemi aziendali. La presente politica viene riesaminata regolarmente per identificare eventuali modifiche che la influenzano e per accertarsi che permanga idonea alle finalità dell'organizzazione e alle aspettative degli stakeholders.

Novara, 23/08/2024

La Direzione