GRUPPO ZENIT

Politiche generali per la qualità e la sicurezza delle informazioni

Gruppo Zenit S.r.l. (di seguito Gruppo Zenit) ha predisposto una **Politica della Qualità e della Sicurezza delle Informazioni** allo scopo di definire la direzione strategica, i principi, le regole di base e gli obiettivi per la gestione della qualità e della sicurezza delle informazioni.

Gruppo Zenit, sviluppando e mantenendo il proprio Sistema, garantisce e salvaguarda la propria brand identity e la propria attività di business stabilendo con precisione ruoli e responsabilità, implementando soluzioni e predisponendo investimenti atti a garantire sicurezza e protezione del proprio sistema informativo, riducendo il rischio di incidenti.

Il **Sistema di Gestione della Qualità, della Sicurezza e della Sicurezza delle Informazioni** si dispiega su tre ambiti in stretta correlazione tra di essi:

- Il **Sistema di Gestione della Qualità** ha l'obiettivo di definire quali strategie applicare per il continuo miglioramento della Qualità, definendo e migliorando i processi aziendali per un coordinamento efficiente ed efficace, orientando l'operatività alla collaborazione con Clienti e Fornitori oltre che con i membri del Team di Gruppo Zenit. Inoltre, internamente all'organizzazione, viene promossa una cultura orientata al continuo miglioramento, aperta a suggerimenti anche attraverso il coinvolgimento di tutto il personale e alla responsabilizzazione dei singoli. Tale processo è rafforzato dalla continua formazione e dal continuo aggiornamento di tutti i dipendenti e collaboratori. A tali obiettivi di Qualità si aggiunge la presa di coscienza e la gestione attenta, previa analisi effettuata internamente, dei rischi derivanti dall'erogazione di servizi IT, al fine di assicurare Sicurezza ambientale e informatica presso tutte le Business Unit aziendali.
- Il **Sistema di Gestione per la Sicurezza** ha l'obiettivo di promuovere attività di sicurezza al fine di definire i principi generali alla protezione delle informazioni, promuovendo attività per il presidio constante di sicurezza delle persone e degli asset nel rispetto delle normative cogenti applicabili in modo da ridurre il rischio di eventi avversi sul patrimonio informativo. Tale Sistema è incluso nel processo ITIL CSI (Continual Improvement) e, pertanto, viene rispettato dal personale, dai clienti e dai fornitori.
- Il **Sistema di Gestione per la Sicurezza delle Informazioni** ha l'obiettivo di definire come mitigare i rischi di Sicurezza delle Informazioni in termini di Riservatezza[1], Integrità[2] e Disponibilità[3].

Le policy riguardano l'erogazione dei servizi IT in modalità gestita (MSP Managed Services Provider) su infrastrutture "Private Cloud" con monitoraggio H24, SPOC H24 Incident e Problem Management, Change Management, erogazione ed assistenza di soluzioni Cloud in modalità IaaS, PaaS, SaaS e consulenza in ambito IT per la Digital Transformation.

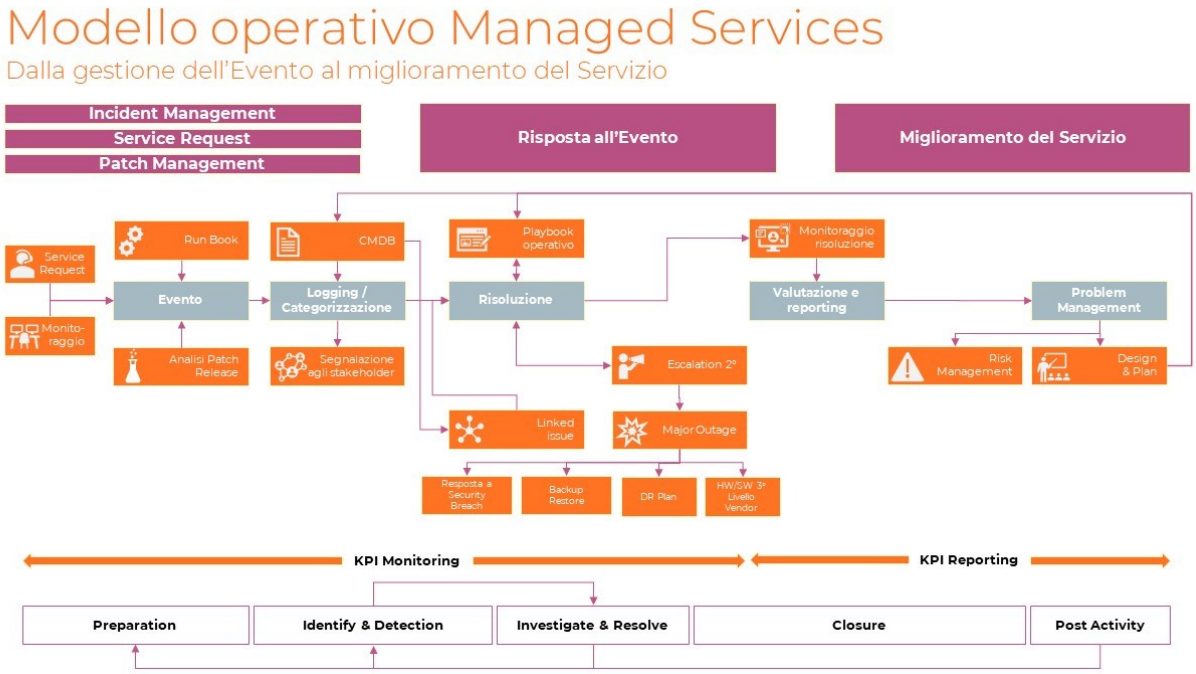
Nel caso in cui le regole di sicurezza stabilite siano disattese da dipendenti, consulenti e/o collaboratori dell'Azienda, l'Amministrazione di Gruppo Zenit si riserva di adottare, nel pieno rispetto dei vincoli di legge e contrattuali, le misure più opportune nei confronti dei soggetti trasgressori.

I soggetti esterni che intrattengono rapporti con Gruppo Zenit devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un

[1] La proprietà dell'informazione di essere nota solo a chi ne ha i privilegi.
[2] La proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi.
[3] La proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che godono dei privilegi di accesso.

"patto di riservatezza" all'atto del conferimento dell'incarico nel caso in cui questo tipo di vincolo non sia espressamente citato nel contratto.

Operational Framework Gruppo Zenit



All'interno dei processi erogati dalla funzione IT Solution di Gruppo Zenit vengono distinti gli **Incident** - intesi come interruzioni momentanee dei servizi verso cui si interviene a livello di Incident Management - dalle **Service Request** o **Change Request** richieste del cliente che non rappresentano una situazione di service disruption e che sono invece gestite tramite una procedura approvativa quale la **Service Request Management**.

Gestire la sicurezza delle informazioni

Obiettivi e misurazione

Il **Sistema di Gestione della Sicurezza delle Informazioni** di Gruppo Zenit è implementato allo scopo di dimostrare agli stakeholders la propria capacità di fornire con regolarità servizi informatici sicuri, massimizzando gli obiettivi di sicurezza e minimizzando il rischio di perdita di riservatezza integrità e disponibilità dei dati gestiti, pianificando e gestendo le attività a garanzia della continuità di servizio, in accordo con il processo di **Valutazione e Trattamento del Rischio**. Tale valutazione è costantemente sottoposta ad analisi e aggiornamento.

L'implementazione del Sistema vuole porsi alla base di un processo di miglioramento continuo mediante revisione periodica delle sue componenti in termini di adeguatezza, efficacia e applicabilità. Il miglioramento continuo è garantito, anche, dall'aggiornamento della documentazione di tipo Controlling, Evidenze e Riferimenti documentali, oltre che mediante il costante aggiornamento e la formazione del personale di Gruppo Zenit.

Responsabilità

- **Amministratore Unico**, con il supporto di Quality&Compliance Manager, è responsabile di garantire che il SGQSI sia implementato e mantenuto conforme a questa politica e di garantire che tutte le risorse necessarie siano disponibili anche attraverso il riesame degli obiettivi generali del SGSI e della definizione di nuovi obiettivi, secondo le linee guida concordate nel contesto dell'**Applicabilità dei Controlli** e secondo la frequenza indicata nelle **Tabelle di Controllo Esecuzione Controlli**.
- **Quality&Compliance Manager** ed **Head of IT Managed Solution** sono responsabili del coordinamento operativo del SGSI e della stesura dei rapporti sulle prestazioni del SGSI.
- **Quality&Compliance Manager** riesamina il SGQSI almeno una volta all'anno o ogni volta che si verifica un cambiamento significativo e prepara il rapporto riassuntivo della riunione per il Riesame della Direzione. Lo scopo del riesame della direzione è stabilire l'idoneità, l'adeguatezza e l'efficacia del SGQSI.
- **Quality&Compliance Manager** e **Head of IT Managed Solutions** sono responsabili di registrare i dati sui metodi di misurazione, la periodicità ed i risultati, per darne evidenza all'Amministrazione Unico e al Responsabile di Amministrazione nel SAL Quality. Il processo di selezione dei controlli della sicurezza delle informazioni (protezioni) è definito nel documento di **Valutazione e Trattamento del Rischio**. I controlli selezionati e il loro stato di implementazione sono elencati nel documento di **Applicabilità dei Controlli**.
- **Comunicazione Interna**, con il supporto di Quality&Compliance Manager, implementa programmi di formazione sulla sicurezza delle informazioni e di sensibilizzazione per i dipendenti. Inoltre, assicura che tutti i dipendenti di Gruppo Zenit, oltre alle parti interessate pertinenti, abbiano familiarità con le Politiche Generali tramite eventi di formazione interna e comunicazioni.

Supporto nell'implementazione del SGSI

Al fine di garantire l'implementazione e il continuo aggiornamento del Sistema l'Amministratore Unico ha manifestato pieno supporto mediante la predisposizione delle risorse necessarie e adeguate alla buona riuscita del progetto: investimento nella formazione e aggiornamento; mantenimento delle strutture fisiche per offrire un adeguato livello di sicurezza proporzionale ai rischi; acquisto di Equipment e Presidi di sicurezza; individuazione di un team dedicato con le relative responsabilità.

16 marzo 2023