



La Sicurezza delle Informazioni si ottiene applicando un complesso set di controlli indicati dalla norma ISO/IEC 27001:2022 ed impostando con costanza ed efficacia Politiche, Processi, Procedure, Strutture organizzative, Funzionalità hardware e software ed un costante monitoraggio per il miglioramento continuo.

La continuità operativa è invece solida e ben fondata in quanto concepita e implementata in accordo allo Standard ISO 22301:2019. Questo consente a FINWAVE di garantire sempre l'adeguata resilienza a fronte del verificarsi di eventi avversi, incluse situazioni di crisi o di emergenza generali, che possono portare all'interruzione della loro erogazione.

Pertanto la sicurezza delle informazioni e la continuità operativa sono responsabilità gestionali, e non un fattore esclusivamente tecnologiche, ancor più in settore strategico quale quello delle financial solutions, del credit management e dei servizi in ambito compliance e regolatorio. Con questa convinzione accompagnata dalla esigenza costante di ricerca di nuove strategie di mercato volte a dare garanzie, non soltanto sulla qualità dei servizi erogati, ma anche sulle modalità di trattamento delle informazioni riguardanti clienti, fornitori e altre parti interessate, oltre che della propria struttura organizzativa, FINWAVE ha deciso e sostiene l'implementazione del SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) modellato sulla base dello standard ISO 27001 integrato con la Gestione della Continuità operativa in accordo allo Standard ISO 22301:2019.

Il SGSI, integrato e conforme anche alla Norma ISO 22301:2019 mutuando la pluriennale esperienza gestionale e le expertise verticali delle Divisioni FINWAVE, attualmente copre le attività erogate nei seguenti campi, uniti dalla strategia di facilitare in modo omnicomprensivo la digitalizzazione end-to end dei propri clienti bancari e aziendali:

- Sviluppo di soluzioni software, applicazioni web e supporto tecnico per il mondo del factoring;
- Progettazione, sviluppo e commercializzazione di soluzioni software per il settore finanziario e del credito e relativi servizi di manutenzione e supporto;
- Attività erogate nel campo dell'Information and Communication Technology e nella Consulenza di Processo, con particolare accento su quelle di progettazione e sviluppo di soluzioni applicative multipiattaforma nel settore Finance, Banking, Financial Market e Insurance;
- Erogazione di prodotti e servizi software inerenti la compliance e gli aspetti regolatori in ambito aziendale e bancario.

Infatti FINWAVE in questa ottica ambisce a conseguire e mantenere il possesso dei requisiti del livello più elevato, in termini di qualità, di sicurezza, di privacy e cybersecurity connessi ai servizi erogati, si prefigge la finalità di proteggere da tutte le minacce - interne o esterne, intenzionali o accidentali - il patrimonio informativo aziendale, ivi comprese le informazioni e i dati relativi a clienti e fornitori; inoltre FINWAVE si prefigge la finalità di mantenere e dimostrare la correttezza delle trattative con clienti e fornitori e di dare evidenza che i servizi erogati non causino direttamente un aumento dei rischi per i clienti.

Per il perseguimento di tali finalità, FINWAVE ha individuato nella documentazione del Sistema di Gestione per la Sicurezza delle Informazioni e della Continuità operativa le corrette modalità di valutazione e i criteri di gestione dei rischi, valutando gli investimenti economici che

l'implementazione e il mantenimento del Sistema di Gestione integrato potrà implicare.

Questo comporta necessariamente il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta e con alto grado di continuità e affidabilità;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali

Pertanto, FINWAVE si impegna, nel rispetto dei requisiti cogenti ad assicurare che:

- le informazioni siano protette da accessi non autorizzati, anche ricorrendo alla crittografia di dati e comunicazioni;
- le informazioni non vengano rivelate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;
- venga minimizzato costantemente il rischio di perdita e/o indisponibilità dei dati gestiti, programmando 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, sorvegliando con continuità il corretto funzionamento degli asset aziendali al fine di rilevare eventi anomali, incidenti e vulnerabilità dei sistemi informativi vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- vengano sempre garantiti la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite e testate;
- il Personale riceva addestramento sulla sicurezza delle informazioni;
- l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da parte di personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto dei più avanzati livelli di sicurezza disponibili;
- tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati;
- si cerchi sempre, nelle scelte progettuali, operative, di partnership e di procurement di inserire a pieno titolo opportuni criteri e principi di responsabilità sociale d'impresa, il rispetto

dei criteri ESG con particolare riferimento alla minimizzazione degli impatti ambientali e alla sostenibilità dei propri processi.

FINWAVE inoltre si impegna a perseguire, in modo sistematico e pianificato, specifici obiettivi (anche declinati per singolo cliente, servizio o cluster di clienti) di continuità operativa.

Tali obiettivi, per i Servizi erogati dalle Divisioni di FINWAVE possono includere:

- obiettivi minimi di continuità operativa;
- obiettivi inerenti il tempo di recupero;
- obiettivi inerenti le attività di controllo operativo e di testing;
- obiettivi di continuità operativa per gli asset critici per l'erogazione dei nostri servizi, includendo in questa filiera la catena di approvvigionamento.

Attraverso l'attuazione di questa politica FINWAVE intende ottemperare all'impegno di conformità a ISO 27001:2022 e ISO 22301:2019 nonché conseguire e mantenere tali certificazioni. Per il conseguimento di tale obiettivo, la direzione di FINWAVE si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da stagisti, collaboratori esterni, consulenti, fornitori sotto contratto, con particolare agli outsourcer che siano in qualsiasi modo coinvolti con le informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni e per la Continuità operativa.

La direzione di FINWAVE si impegna infine a riesaminare regolarmente la politica ed eventuali modifiche che la influenzino, per accertarsi che permanga idonea all'attività e alla capacità di FINWAVE di soddisfare i Clienti, i Fornitori e le altre parti interessate.

Milano, 09/05/2024

La Direzione

FINWAVE SPA

