POLITICA INTEGRATA - SICUREZZA DELLE INFORMAZIONI E CONTINUITA' OPERATIVA

ETICHETTATURA	
☐	RISERVATO
☐	INTERNO
☒	PUBBLICO

CLASSIFICAZIONE	
☐	COPIA CONTROLLATA
☒	COPIA NON CONTROLLATA

POLITICA INTEGRATA - SICUREZZA DELLE INFORMAZIONI E CONTINUITA' OPERATIVA

ED.	REV.	CAUSALE	DATA
2	1	Revisione	22.02.2023
2	2	Implementazione	09.09.2024

Elaborazione

(RSGI)

Emissione

(Direzione)

PREMESSA

LADISA S.R.L. è una società che opera principalmente nel settore di EROGAZIONE DI SERVIZI DI RISTORAZIONE COLLETTIVA PER ENTI PUBBLICI E PRIVATI: MENSE SCOLASTICHE, SANITARIE, MILITARI E DELLA PUBBLICA SICUREZZA. PREPARAZIONE, CONFEZIONAMENTO IN MONOPORZIONE E MULTIPORZIONE, TRASPORTO E DISTRIBUZIONE PASTI. PIATTAFORMA CENTRALIZZATA PER ACQUISTO, TRASPORTO, DISTRIBUZIONE E COMMERCIALIZZAZIONE DI MERCI (NO FOOD) E DERRATE ALIMENTARI PER LA RISTORAZIONE COLLETTIVA E LA GRANDE DISTRIBUZIONE ORGANIZZATA. Data la natura delle proprie attività, **LADISA S.R.L.** considera la sicurezza delle informazioni e la continuità operativa un fattore irrinunciabile per la protezione del proprio patrimonio informativo.

LADISA S.R.L. pone particolare attenzione ai temi riguardanti la sicurezza dei dati e la continuità operativa durante il ciclo di vita di progettazione e sviluppo dei propri servizi, che devono essere ritenuti un bene primario dell'azienda.

Su tali basi **LADISA S.R.L** ha deciso di porre in essere un Sistema di Gestione integrato per la Sicurezza delle Informazioni (SGSI) e per la continuità operativa (SGCO) definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità alle indicazioni della norma **ISO/IEC 27001:2022 e UNI EN ISO 22301:2019.**

OBIETTIVI

Il Sistema Informativo (inclusivo delle risorse tecnologiche, hardware, software, informazioni in qualsiasi formato, dati, documenti, reti telematiche e delle risorse umane dedicate alla loro amministrazione, gestione e utilizzo) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi di **LADISA S.R.L.**, in considerazione della criticità dei processi aziendali che dipendono da esso. Il presente documento ha l'obiettivo di definire le politiche sui sistemi informativi e la policy sulla sicurezza delle informazioni e sulla continuità operative al fine di sviluppare un efficiente e sicuro Sistema di Gestione integrato attraverso il rispetto delle seguenti proprietà:

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

L'osservanza dei livelli di sicurezza stabiliti da **LADISA S.R.L.** attraverso l'implementazione dell'SGSI, permette di:

- preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- proteggere al meglio il patrimonio informativo proprio e dei propri clienti;
- aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi di sicurezza dei dati
- rispondere pienamente alle indicazioni della normativa vigente e cogente e degli standard internazionali di sicurezza dei dati.

AMBITO DI APPLICAZIONE

La politica integrata per la sicurezza delle informazioni e la continuità operativa adottata da **LADISA S.R.L** si applica indistintamente a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolti. La Politica deve costituire un approccio Sistematico alla sicurezza delle informazioni e alla continuità operativa per tutti i componenti dell'organizzazione che – a qualsiasi Titolo – possono intervenire su qualsiasi informazione presente all'interno dell'Azienda, nell'ambito dei servizi erogati.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di **LADISA S.R.L** rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

Il patrimonio informativo della **LADISA S.R.L** da tutelare è costituito dall'insieme delle informazioni localizzate nella sede dell'azienda.

Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- ☐ Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

- ☐ Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- ☐ Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- ☐ Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- ☐ Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- ☐ È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- ☐ Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- ☐ Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- ☐ Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- ☐ Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'attività di **LADISA S.R.L**, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine aziendale.

POLITICA PER LA BUSINESS CONTINUITY

La continuità operativa è assicurata nell'operatività aziendale e nei servizi erogati ai Clienti ed è mantenuta attraverso un processo ben definito sottoposto a revisione annuale e secondo necessità.

Il Sistema di Gestione integrato per la Sicurezza delle informazioni e per la Continuità Operativa è implementato e mantenuto secondo i requisiti specificati dall'insieme di procedure operative aziendali e sottoposto a revisione su base periodica regolare per garantirne la conformità ad obblighi di legge, regolamenti e norme volontarie applicate.

Attraverso tale insieme di procedure, sono:

- identificati i processi, i servizi e i fattori coinvolti nell'erogazione, valutati per criticità e documentati sulla base di requisiti normativi, contrattuali, delle esigenze di business e delle regole interne;
- effettuate dall'organizzazione, periodicamente e regolarmente, analisi di impatto sulle attività operative (BIA Business Impact Analysis) e analisi dei rischi sui servizi erogati che rientrano nel perimetro del sistema di gestione integrato;
- stabiliti, documentati e testati periodicamente i Piani di continuità operativa e di Disaster recovery, assicurando l'efficacia e l'aggiornamento continuo delle soluzioni tecniche e organizzative adottate.

Il personale è adeguatamente formato sulla politica per la continuità operativa affinché contribuisca

consapevolmente e responsabilmente alla sua applicazione e al miglioramento continuo del sistema. A tale scopo, è garantita l'adeguatezza e l'aggiornamento periodico e regolare dei piani di formazione per il personale e altre eventuali entità coinvolte, ad esempio, parti terze e subappaltatori con un ruolo critico nell'erogazione dei servizi che devono essere informati e conformi alle politiche di continuità operativa adottate.

Rispetto al verificarsi di un evento di crisi che possa causare un'interruzione dei servizi critici, la Direzione di LADISA S.R.L ha proposto e approvato i seguenti obiettivi strategici generali:

- ☐ garantire la salvaguardia e sicurezza fisica delle persone;
- ☐ garantire la continuità operativa e minimizzare gli impatti sul business, assicurando un rapido ripristino del normale stato di svolgimento delle attività e di erogazione dei servizi;
- ☐ migliorare la capacità di resistere ad incidenti (la resilienza) delle proprie architetture;
- ☐ tutelare il valore aziendale;
- ☐ garantire disponibilità e livello di servizio ai Clienti e alle altre parti interessate, assicurando conformità ai requisiti contrattuali e soddisfazione delle necessità;
- ☐ garantire la conformità alle prescrizioni di legge e di regolamentazione e ai vincoli di natura contrattuale;
- ☐ garantire la pianificazione e assicurazione della disponibilità delle risorse (materiali, umane e in termini di quantità e competenza);
- ☐ garantire attività di formazione;
- ☐ garantire il monitoraggio delle performance ed il continuo miglioramento del sistema di gestione;
- ☐ assicurare simulazioni, test ed esercitazioni al fine di garantire l'efficacia dei Piani di BC e DR.

La pianificazione degli obiettivi determina le attività che devono essere effettuate, le responsabilità di attuazione, i tempi di completamento, le risorse necessarie e le modalità di verifica dei risultati.

LADISA S.R.L. ha fissato obiettivi specifici e tattici, misurabili per i singoli elementi di Business Continuity, ossia per i piani, per le esercitazioni, simulazioni e test, per il mantenimento, che sono definiti e documentati nelle procedure:

- Obiettivi– Recovery Time Objectives (RTO),

- Recovery Point Objectives (RPO),
- obiettivi minimi di continuità operativa (MBCO)
- obiettivi di esercitazioni e di test.

Per garantire il raggiungimento di tali obiettivi di continuità operativa, la Direzione ha adottato le seguenti principali misure di controllo:

- ☐ **misure di controllo del rischio**, finalizzate alla mitigazione e al contenimento sia relativamente alla probabilità di accadimento di eventuali incidenti, sia per la capacità di impatto. La Metodologia di Valutazione e il Trattamento del Rischio adottata da **LADISA** identifica gli elementi di rischio che possono mettere a repentaglio il ripristino dell'operatività e definisce i livelli di rischio accettabili sia per la ISO 22301:2019 che, in ambito sicurezza delle informazioni, per la ISO 27001:2022. Le misure di resilienza sono atte a ripristinare i processi in maniera sufficientemente veloce da evitare conseguenze negative;
- ☐ la **Business Impact Analysis** (BIA) identifica, quantifica e qualifica i processi e i servizi critici determinanti ai fini della continuità operativa aziendale, determinando gli impatti che potrebbero essere causati in caso di indisponibilità delle risorse assegnate a tali processi/servizi;
- ☐ Il **Piano per la Continuità** delle Attività aziendali (Business Continuity Plan) che considera i rischi identificati e le strategie per contrastarli, minimizzando l'interruzione del lavoro e assicurando un rapido ripristino delle attività;
- ☐ Il **Piano di Disaster Recovery** che permette a **LADISA** di affrontare eventi avversi, garantendo il ripristino dei servizi critici in tempi e con modalità che limitano le conseguenze dell'impatto negativo;
- ☐ La **Procedura di Gestione degli Incidenti**, adeguata a riconoscere, comunicare e rispondere agli incidenti in un modo efficace ed appropriato contenendone l'impatto

RESPONSABILITÀ DELLA POLITICA INTEGRATA SICUREZZA DELLE INFORMAZIONI E CONTINUITA' OPERATIVA

La direzione sostiene attivamente la sicurezza delle informazioni e la continuità operativa in azienda tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni ed alla continuità operativa e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGI;
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del SGI;

- controllare che il SGI sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni e la continuità operativa;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni e della continuità operativa;
- attuare, sostenere e verificare periodicamente la presente Politica, e divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa;
- riesaminare periodicamente gli obiettivi e la Politica per accertarne la continua idoneità.

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza di questa Politica e della segnalazione di anomalie di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti con **LADISA S.R.L.**, devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

RIESAME DELLA POLITICA

La presente Politica Aziendale sarà revisionata periodicamente sia in caso di eventi esterni, quali ad esempio modifiche della normativa esterna ovvero indicazioni delle Autorità, sia di modifiche organizzative ed operative che abbiano impatto sui Sistemi Informativi, sulla continuità operativa e sulla sicurezza delle informazioni.

La presente Politica verrà comunque riconfermata e sottoscritta con cadenza annuale. La sua sottoscrizione avverrà durante l'attività di Riesame della Direzione del SGI.

09.09.2024

Direzione