

SISTEMA DI GESTIONE PER LA BUSINESS CONTINUITY

DOPOR

Documento Politica per la sicurezza e Resilienza

Codice DOC: 02DIBC**Livello di riservatezza 0 - Pubblico**
Informazioni di pubblico accesso.

Dati pubblicati su internet o destinati alla pubblica diffusione.

Revisione	Data di revisione	Redatta da	Verificata da	Approvata
Rilascio 1.0 Prima stesura	Febbraio 2023	RRSI Elena Amendola	RSGSI Daniel Bizzarro	DD Valerio Bizzarro

Lista di distribuzione: Pubblicazione su sito web aziendale**A:**

Al personale Data Vision

	SGBC Documento Politica per la Business Continuity	02DIBC	
		Rev. 1.0	
		Data: Feb 2023	Pag. 3 di 6

1. SCOPO, CAMPO DI APPLICAZIONE E DESTINATARI

Lo scopo di questo documento è definire l'obiettivo, il campo di applicazione e le regole di base per la gestione della Business Continuity, è identificando i rischi potenziali dell'organizzazione.

Data Vision ha definito ed implementato un Sistema di Gestione per la Business Continuity (SGBC), basato sui requisiti definiti dallo standard ISO 22301:2019 (Security and Resilience – Business continuity management systems) sul perimetro costituito dalle attività di progettazione e sviluppo di soluzioni applicative software e relativa assistenza e di erogazione di consulenza e servizi a supporto dei Clienti.

La presente Politica è applicata a tutte le strutture, attività, prodotti e servizi nel campo di applicazione del Sistema di Gestione della Business Continuity (SGBC). Sono inclusi i due seguenti siti aziendali

- la sede centrale di Data Vision;
- il sito di Disaster recovery.

I destinatari di questo documento sono tutti i dipendenti di Data Vision, così come tutti i fornitori, i partner dei servizi in outsourcing, i clienti e tutti quelli che sono coinvolti nella gestione della Business Continuity.

La presente Politica copre ogni aspetto della sicurezza delle informazioni (ISO 27001:2019) della gestione della continuità operativa. La responsabilità della gestione di questo documento è del Responsabile del Sistema di Gestione per la Continuità Operativa.

2. IMPEGNO

L'Alta Direzione si impegna a soddisfare i requisiti di tutte le parti interessate e a migliorare continuamente il SGBC. L'impegno della Direzione si attua

- a) assicurando che siano stabiliti la politica e gli obiettivi per la continuità operativa e che essi siano compatibili con gli indirizzi strategici dell'organizzazione;
- b) assicurando l'integrazione dei requisiti del SGBC nei processi di business dell'organizzazione;
- c) assicurando la disponibilità delle risorse necessarie al SGBC, tramite la messa a disposizione dei mezzi tecnici, economici e delle risorse umane necessarie;
- d) comunicando l'importanza di una continuità operativa aziendale efficace e del mantenimento della conformità ai requisiti del SGBC;
- e) assicurando che il SGBC consegua i risultati attesi;
- f) guidando e supportando il personale affinché contribuisca con impegno quotidiano all'efficacia del SGBC;
- g) promuovendo il miglioramento continuo;
- h) fornendo supporto agli altri ruoli manageriali rilevanti per dimostrare la loro leadership e il loro impegno nelle rispettive aree di responsabilità.
- i) verificata periodicamente dalla Direzione, nel corso del riesame del SGBCO.

3. LA 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 per la Continuità Operativa è implementato e mantenuto secondo i requisiti specificati dall'insieme di procedure operative di Business Continuity aziendale 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

	SGBC Documento Politica per la Business Continuity	02DIBC	
		Rev. 1.0	
		Data: Feb 2023	Pag. 4 di 6

- 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 SGBC, secondo un processo definito e documentato che rientra nell'ambito della Sicurezza delle Informazioni (ISO 27001:2019);
- 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 SGBC. 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 Data Vision 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
- 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. Data Vision 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 precedentemente citate del SGBC:

- 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 Data vision 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 27001:2019.

	SGBC Documento Politica per la Business Continuity	02DIBC	
		Rev. 1.0	
		Data: Feb 2023	Pag. 5 di 6

- 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 Data Vision di affrontare eventi avversi, garantendo il ripristino dei servizi critici in tempi e con modalità che limitano le conseguenze dell'impatto negativo.
- La Procedure di Gestione degli Incidenti, adeguata a riconoscere, comunicare e rispondere agli incidenti in un modo efficace ed appropriato contenendone l'impatto.

3.1. COMUNICARE LA POLITICA PER LA CONTINUITÀ OPERATIVA

La politica per la continuità operativa è

- a) resa disponibile come informazione documentata;
- b) comunicata all'interno dell'organizzazione;
- c) resa disponibile alle parti interessate, per quanto appropriato.

La comunicazione della presente Politica è effettuata all'interno dell'azienda, ma anche – se è necessario – a parti interessate. Il RSG è responsabile della comunicazione.

Allo scopo, la presente Politica è comunicata a tutti i dipendenti e collaboratori e pubblicata integralmente sul sito aziendale a disposizione delle parti interessate.

La Direzione e il Responsabile del SGBC devono assicurare che la Politica per la Continuità Operativa sia compresa ed attuata da tutto il personale nello svolgimento della propria attività. In caso di cambiamenti a qualsiasi livello, sono valutati gli impatti sulla sicurezza delle informazioni, garantendone la completa ed efficace gestione.

4. RUOLI, RESPONSABILITÀ E AUTORITÀ

La Direzione assicura che le responsabilità e le autorità per i ruoli pertinenti siano assegnate e comunicate all'interno dell'organizzazione. A tale scopo, la Direzione ha definito e formalizzato la struttura organizzativa, i ruoli e le responsabilità nell'ambito della gestione della continuità operativa, promuovendo il coinvolgimento di tutte le funzioni aziendali. La Direzione ha assegnato le responsabilità e autorità per

- a) assicurare che il SGBC sia conforme ai requisiti del presente documento;
- b) riferire alla Direzione sulle prestazioni del SGBC.

Data Vision prima di eseguire le modifiche necessarie al SGBC, garantisce lo scopo e considera le conseguenze potenziali dei cambiamenti proposti. Il Responsabile del SGBC si occupa di pianificare eventuali cambiamenti necessari al SGBC; di svolgere esercitazioni, di testare ogni disposizione legata alla BC e di preparare un report di tali attività; di monitorare eventuali non conformità, falsi allarmi, incidenti, ecc.; si impegna, inoltre, a misurare i risultati e il raggiungimento degli obiettivi almeno una volta all'anno durante l'Audit interno e ha la responsabilità del Riesame periodico. Gli obiettivi e i corrispondenti risultati sono rivisti dalla Direzione di Data Vision almeno una volta all'anno durante il Riesame della Direzione, attraverso metodi di misurazione documentati.

	SGBC Documento Politica per la Business Continuity	02DIBC	
		Rev. 1.0	
		Data: Feb 2023	Pag. 6 di 6

L'attuazione della presente Politica per la Business Continuity è sottoposta in modo trasparente alla verifica dei Clienti, ed eventuali altre parti interessate, ed è controllata in modo oggettivo da un Ente di Certificazione indipendente.

La Direzione, condividendo i Principi e gli Obiettivi per una corretta politica finalizzata alla sicurezza e alla resilienza operativa, approva ed emette il presente documento di Politica per la Business Continuity e supporta pienamente il programma per l'attuazione e mantenimento, richiamando su questi aspetti l'attenzione del proprio personale, dei collaboratori, fornitori e clienti.