SISTEMA DI GESTIONE PER LA BUSINESS CONTINUITY

DATA VISION S.R.L.

Documento Politica per la Continuità Operativa,

il Ripristino in caso di Disastro e la Gestione delle Crisi

La presente politica costituisce una delle politiche di sicurezza informatica per l'ambito "h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi", richiesto dalla Determinazione ACN n. 164179/2025, Allegato 1, in attuazione della misura GV.PO-01 – requisiti ID.IM-04. Documento aggiornato a partire dal documento 02DIBC – DOPOR rev. 1.1 (Gen 2024), adeguato ai requisiti NIS2 / Determinazione ACN n. 164179/2025 in data Giugno 2026.

Codice DOC: 02DI-BC_POL-008
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 2.0 Adeguamento NIS2 (ACN 164179/2025, ambito h) Modifica della codifica (ex DOPOR)	Ottobre 2026	RRSG Elena Amendola	RSG/RSQ Daniel Bizzarro	RDSG **/** PdC NIS2 Valerio Bizzarro

Lista di distribuzione: Pubblicazione su sito web aziendale
A:
Al personale Data Vision

Cronologia delle revisioni				
Revisione	**Data di revisione**	**Redatta da**	**Verificata da**	**Approvata**
Rilascio 1.1 Aggiornamento ISO 27001	Gennaio 2024	RRSG Elena Amendola	RSG Daniel Bizzarro	RDSG Valerio Bizzarro
Rilascio 1.0 Prima stesura	Febbraio 2023	RRSI Elena Amendola	RSG Daniel Bizzarro	RDSG Valerio Bizzarro

SOMMARIO

1. Scopo, campo di applicazione e destinatari 4
2. Riferimenti normativi 4
3. Terminologia ed abbreviazioni 5
4. Impegno della Direzione....5
5. La Politica per la Continuità Operativa, il Ripristino in caso di Disastro e la Gestione delle Crisi 6
5.1. Piano di Continuità Operativa (BCP)....6
5.2. Piano di Ripristino in caso di Disastro (DRP)....7
5.3. Piano di Gestione delle Crisi 7
5.4. Approvazione e riesame dei piani 7
5.5. Formazione e consapevolezza 7
5.6. Obiettivi strategici 8
5.7. Obiettivi specifici e misurabili....8
5.8. Misure di controllo 8
5.9. Comunicare la Politica per la Continuità Operativa, il DR e la Gestione delle Crisi....9
6. Ruoli, responsabilità e autorità 10
6.1. Direzione / organi di amministrazione e direttivi (DD)....10
6.2. Punto di Contatto NIS2 / Referente CSIRT (Valerio Bizzarro)....10
6.3. Responsabile del Sistema di Gestione per la Business Continuity – RSGBC (Daniel Bizzarro) 10
6.4. Amministratore Sistemi / Responsabile BC-DR (Luca Urbinati) 10
6.5. CSM / Responsabile Gestione Rischi (Elena Amendola)....11
7. Verifica, riesame e miglioramento continuo....11

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, del ripristino in caso di disastro (Disaster Recovery) e della gestione delle crisi, 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 (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.

Dal 12 aprile 2025, con Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Data Vision S.r.l. è stata inserita nell'elenco dei soggetti NIS ai sensi dell'articolo 7, comma 3, lettera a) del Decreto legislativo 4 settembre 2024, n. 138, ed individuata quale soggetto Importante. Ai sensi della misura GV.PO-01 dell'Allegato 1 – "Misure di sicurezza di base per i soggetti importanti" della Determinazione ACN n. 164179/2025, Data Vision adotta e documenta politiche di sicurezza informatica per sedici ambiti, tra cui l'ambito h) "Continuità operativa, ripristino in caso di disastro e gestione delle crisi". Il presente documento costituisce la politica relativa a tale ambito, in attuazione della misura ID.IM-04, ed è complementare e allineato alla Politica per la Sicurezza delle Informazioni, alla Politica di Sicurezza dei Dati e alle altre politiche di sicurezza informatica adottate da Data Vision.

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) e, per quanto attiene ai sistemi informativi e di rete rilevanti individuati ai sensi della misura GV.OC-04, costituisce altresì la politica di riferimento per il piano di continuità operativa, il piano di ripristino in caso di disastro e il piano di gestione delle crisi richiesti dalla misura ID.IM-04. 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, del Disaster Recovery e della gestione delle crisi.

La presente Politica copre ogni aspetto della sicurezza delle informazioni (ISO 27001) della gestione della continuità operativa. La responsabilità della gestione di questo documento è del Responsabile del Sistema di Gestione per la Business Continuity (RSGBC), che si avvale del supporto della funzione Amministratore Sistemi / Responsabile BC-DR per gli aspetti tecnico-operativi.

2. RIFERIMENTI NORMATIVI

- UNI EN ISO 22301 – Security and resilience – Business continuity management systems;
- UNI CEI ISO/IEC 27001 – Sistemi di gestione per la sicurezza delle informazioni;

- Decreto legislativo 4 settembre 2024, n. 138 (recepimento direttiva NIS2);
- Determinazione ACN n. 164179/2025 – Allegato 1 "Misure di sicurezza di base per i soggetti importanti", in particolare misura GV.PO-01 (ambito h, "Continuità operativa, ripristino in caso di disastro e gestione delle crisi") e misura ID.IM-04;
- Framework Nazionale per la Cybersecurity e la Data Protection (FNCS), versione 2025.

3. TERMINOLOGIA ED ABBREVIAZIONI

SGBC: Sistema di Gestione per la Business Continuity di Data Vision.

BIA (Business Impact Analysis): analisi di impatto sulle attività operative, che identifica, quantifica e qualifica i processi e i servizi critici determinanti ai fini della continuità operativa aziendale.

BCP (Business Continuity Plan): Piano di Continuità Operativa.

DRP (Disaster Recovery Plan): Piano di Ripristino in caso di Disastro.

Piano di gestione delle crisi: documento che definisce ruoli, responsabilità e modalità di comunicazione del personale e, se opportuno, dei fornitori, in situazioni di crisi.

RTO (Recovery Time Objective): tempo massimo accettabile entro cui un processo o servizio deve essere ripristinato dopo un'interruzione.

RPO (Recovery Point Objective): punto temporale massimo accettabile a cui i dati devono essere ripristinati dopo un'interruzione.

MBCO (Minimum Business Continuity Objective): livello minimo di servizio accettabile durante un'interruzione per il raggiungimento degli obiettivi di business.

Sistemi informativi e di rete rilevanti: i sistemi individuati da Data Vision ai sensi della misura GV.OC-04, oggetto prioritario dei piani di cui alla presente politica.

DD: Direzione Data Vision / organi di amministrazione e direttivi, cui compete l'approvazione dei piani di cui alla presente politica.

4. IMPEGNO DELLA DIREZIONE

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:

- assicurando che siano stabiliti la politica e gli obiettivi per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi, e che essi siano compatibili con gli indirizzi strategici dell'organizzazione e con la strategia di gestione del rischio di cybersecurity;
- assicurando l'integrazione dei requisiti del SGBC nei processi di business dell'organizzazione;

- assicurando la disponibilità delle risorse necessarie al SGBC, tramite la messa a disposizione dei mezzi tecnici, economici e delle risorse umane necessarie;
- comunicando l'importanza di una continuità operativa aziendale efficace e del mantenimento della conformità ai requisiti del SGBC e della Determinazione ACN n. 164179/2025;
- assicurando che il SGBC consegua i risultati attesi;
- guidando e supportando il personale affinché contribuisca con impegno quotidiano all'efficacia del SGBC;
- promuovendo il miglioramento continuo;
- fornendo supporto agli altri ruoli manageriali rilevanti per dimostrare la loro leadership e il loro impegno nelle rispettive aree di responsabilità;
- approvando, in quanto organo di amministrazione e direttivo, il piano di continuità operativa, il piano di ripristino in caso di disastro e il piano di gestione delle crisi di cui alla misura ID.IM-04, e le relative revisioni;
- verificando periodicamente, nel corso del riesame del SGBC, lo stato di attuazione della presente politica e dei piani ad essa correlati.

5. LA POLITICA PER LA CONTINUITÀ OPERATIVA, IL RIPRISTINO IN CASO DI DISASTRO E LA GESTIONE DELLE CRISI

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 almeno 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, ivi compresi quelli derivanti dalla normativa NIS2. 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, con particolare riferimento ai sistemi informativi e di rete rilevanti individuati ai sensi della misura GV.OC-04;
- 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) e della valutazione del rischio di cybersecurity (misura ID.RA-05);
- stabiliti, documentati e testati periodicamente il Piano di Continuità Operativa, il Piano di Ripristino in caso di Disastro e il Piano di Gestione delle Crisi, secondo gli elementi minimi di cui alla misura ID.IM-04, assicurando l'efficacia e l'aggiornamento continuo delle soluzioni tecniche e organizzative adottate.

5.1. Piano di Continuità Operativa (BCP)

Per almeno i sistemi informativi e di rete rilevanti, è definito, attuato, aggiornato e documentato un Piano di Continuità Operativa, che comprende almeno:

- le finalità, ivi incluse le esigenze di continuità operativa, e l'ambito di applicazione;
- i ruoli e le responsabilità;
- i contatti principali e i canali di comunicazione (interni ed esterni);
- le condizioni per l'attivazione e la disattivazione del piano;
- le risorse necessarie, ivi compresi i backup e le ridondanze.

5.2. Piano di Ripristino in caso di Disastro (DRP)

Per almeno i sistemi informativi e di rete rilevanti, è definito, attuato, aggiornato e documentato un Piano di Ripristino in caso di Disastro, che comprende almeno:

- le finalità, ivi incluse le esigenze di ripristino in caso di disastro, e l'ambito di applicazione;
- i ruoli e le responsabilità;
- i contatti principali e i canali di comunicazione (interni ed esterni);
- le condizioni per l'attivazione e la disattivazione del piano;
- le risorse necessarie, ivi compresi i backup e le ridondanze;
- l'ordine di ripristino delle operazioni;
- le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino (RTO e RPO).

5.3. Piano di Gestione delle Crisi

Per almeno i sistemi informativi e di rete rilevanti, è definito, attuato, aggiornato e documentato un Piano di Gestione delle Crisi, che comprende almeno:

- i ruoli e le responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire;
- le modalità di comunicazione tra i soggetti e le autorità competenti, ivi inclusa, per gli incidenti rilevanti ai fini NIS2, la comunicazione verso il CSIRT Italia tramite il Punto di Contatto NIS2.

5.4. Approvazione e riesame dei piani

Il Piano di Continuità Operativa, il Piano di Ripristino in caso di Disastro e il Piano di Gestione delle Crisi sono approvati dagli organi di amministrazione e direttivi di Data Vision.

I tre piani sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi. Sulla base delle lezioni apprese durante la gestione degli incidenti di sicurezza informatica, i piani sono altresì aggiornati per tenere in considerazione gli insegnamenti maturati e correggere le eventuali criticità riscontrate.

5.5. Formazione e consapevolezza

Il personale è adeguatamente formato sulla politica per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi, 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.

5.6. Obiettivi strategici

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, ivi compresi gli obblighi NIS2, e ai vincoli di natura contrattuale;
- assicurare simulazioni, test ed esercitazioni al fine di garantire l'efficacia dei Piani di BC e DR e del Piano di Gestione delle Crisi.

5.7. Obiettivi specifici e misurabili

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, definiti e documentati nelle procedure operative del SGBC:

- obiettivi di Recovery Time Objective (RTO);
- obiettivi di Recovery Point Objective (RPO);
- obiettivi minimi di continuità operativa (MBCO);
- obiettivi di esercitazioni e di test.

5.8. Misure di controllo

Per garantire il raggiungimento degli obiettivi di continuità operativa, ripristino in caso di disastro e gestione delle crisi, 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 , sia in ambito sicurezza delle informazioni per la ISO 27001 e per la valutazione del rischio di cybersecurity ai sensi della misura ID.RA-05;
- **misure di resilienza,** atte a ripristinare i processi in maniera sufficientemente veloce da evitare conseguenze negative;
- **la Business Impact Analysis (BIA),** che 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;
- **il Piano di Gestione delle Crisi,** che definisce ruoli, responsabilità e modalità di comunicazione interna ed esterna in situazioni di crisi;
- **la Procedura di Gestione degli Incidenti,** adeguata a riconoscere, comunicare e rispondere agli incidenti in un modo efficace ed appropriato, contenendone l'impatto, in coordinamento con il processo di gestione degli incidenti di sicurezza informatica NIS2 (procedura S004).

5.9. Comunicare la Politica per la Continuità Operativa, il DR e la Gestione delle Crisi

La politica per la continuità operativa, il ripristino in caso di disastro e la gestione delle crisi è:

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

La comunicazione della presente Politica è effettuata all'interno dell'azienda, ma anche – se necessario – verso le parti interessate. Il RSGBC 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 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 e sulla continuità operativa, garantendone la completa ed efficace gestione.

6. 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, del ripristino in caso di disastro e della gestione delle crisi, promuovendo il coinvolgimento di tutte le funzioni aziendali.

6.1. Direzione / organi di amministrazione e direttivi (DD)

- approva il Piano di Continuità Operativa, il Piano di Ripristino in caso di Disastro e il Piano di Gestione delle Crisi, e le relative revisioni;
- assicura che il SGBC sia conforme ai requisiti del presente documento e agli obblighi derivanti dalla Determinazione ACN n. 164179/2025;
- è informata, mediante apposite relazioni periodiche, sulle prestazioni del SGBC e sugli esiti dei test e delle esercitazioni.

6.2. Punto di Contatto NIS2 / Referente CSIRT (Valerio Bizzarro)

- approva, in qualità di referente verso gli organi di amministrazione e direttivi, la presente politica e i piani ad essa correlati;
- coordina, in caso di crisi che comporti un incidente di sicurezza informatica significativo ai sensi della normativa NIS2, le comunicazioni verso il CSIRT Italia e l'Agenzia per la Cybersicurezza Nazionale, in coordinamento con il Piano di Gestione delle Crisi.

6.3. Responsabile del Sistema di Gestione per la Business Continuity – RSGBC (Daniel Bizzarro)

- è responsabile della gestione del presente documento e della sua diffusione;
- pianifica eventuali cambiamenti necessari al SGBC, prima di eseguirli garantendone lo scopo e considerando le conseguenze potenziali;
- svolge esercitazioni, testa ogni disposizione legata alla BC e al DR e prepara un report di tali attività;
- monitora eventuali non conformità, falsi allarmi, incidenti, ecc.;
- misura i risultati e il raggiungimento degli obiettivi almeno una volta all'anno durante l'Audit interno e ha la responsabilità del Riesame periodico.

6.4. Amministratore Sistemi / Responsabile BC-DR (Luca Urbinati)

- attua e mantiene tecnicamente il Piano di Continuità Operativa e il Piano di Ripristino in caso di Disastro, ivi inclusa la gestione del sito di Disaster Recovery;
- pianifica, esegue e documenta i test di ripristino e le esercitazioni periodiche;
- coordina, in caso di crisi, le attività tecniche di ripristino dei sistemi informativi e di rete coinvolti.

6.5. CSM / Responsabile Gestione Rischi (Elena Amendola)

- supporta la redazione e l'aggiornamento della presente politica e dei piani correlati;
- conduce e mantiene aggiornata la Business Impact Analysis (BIA) e la valutazione del rischio di cybersecurity (ID.RA-05) propedeutiche ai piani di cui alla presente politica;
- monitora la coerenza tra gli obiettivi di continuità operativa (RTO, RPO, MBCO) e i livelli di rischio accettabili definiti da Data Vision.

7. VERIFICA, RIESAME E MIGLIORAMENTO CONTINUO

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.

L'attuazione della presente Politica 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 per quanto attiene la conformità alla norma ISO 22301 .

In conformità ai requisiti legislativi NIS2 (misura GV.PO-02), la presente politica e i relativi piani sono comunque riesaminati e, se opportuno, aggiornati periodicamente e almeno con la frequenza indicata al paragrafo 5.4, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

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 e supporta pienamente il programma per l'attuazione e mantenimento, richiamando su questi aspetti l'attenzione del proprio personale, dei collaboratori, fornitori e clienti.