Piano di Continuità Operativa / Estratto

Il presente documento, il cui scopo è la distribuzione pubblica, è un estratto del Business Continuity Plan Master Chart, che delinea gli aspetti organizzativi e tecnologici messi in atto per assicurare la continuità dei processi core in caso di eventi interruttivi inattesi.
Master Chart si propone di fornire servizi sicuri ed efficienti ai propri clienti e ai mercati in cui opera. Al fine di raggiungere tale obiettivo, si impegna a dare la massima priorità al mantenimento della continuità dei servizi di compensazione, supportati dalla propria infrastruttura tecnica, dalle applicazioni operative essenziali, dalle infrastrutture fisiche e dal personale.

1. Scopo e Obiettivi

Questo piano definisce le strategie e le procedure per garantire la continuità dei servizi offerti da Master Chart in caso di guasti tecnici, cyber attacchi o eventi imprevisti. L'obiettivo è:

- Ridurre al minimo l'impatto di interruzioni operative.
- Garantire il rispetto degli SLA con i clienti.
- Assicurare la protezione e il ripristino rapido dei dati.

2. Ambito di Applicazione

Il piano si applica a:

- Software e applicazioni: backend, API, frontend.
- Sistemi installati presso i clienti
- Infrastruttura cloud: database, server, bilanciatori di carico.
- Sicurezza IT: protezione da minacce informatiche e perdita dati.
- Supporto clienti: gestione delle comunicazioni in caso di emergenza.

3. Governance e Ruoli

La gestione della continuità operativa è affidata al Comitato di Continuità Operativa, composto da:

- CIO (Chief Information Officer) → responsabile della supervisione generale.
- IT Security Manager → gestione delle minacce informatiche.
- Cloud Operations Lead → monitoraggio e failover infrastrutturale.
- Customer Support Lead → comunicazione con i clienti in caso di interruzioni.

MASTER CHART S.r.l.
Via Eugenio Montale, 2 - 25087 Salò (BS)
Tel. 0365 / 41778 r.a. Fax 0365 / 40378
C.C.I.A.A. 0345672 Trib. BS 52011
P. IVA e C.F. 01736620988
Indirizzo Internet www.masterchart.it
E-mail info@masterchart.it
Cap. Soc. Euro 100.000,00 i.v.

Ruoli Operativi in caso di emergenza

- Incident Manager: valuta l'emergenza e attiva il piano.
- Team IT Security: analizza e mitiga minacce cyber.
- Team Cloud Ops: esegue il failover e il disaster recovery.
- Responsabile Comunicazioni: aggiorna clienti e stakeholder.

4. Analisi dei Rischi e Impatti (BIA)

Minacce principali

- Guasto hardware/software → perdita temporanea di servizio.
- Attacchi informatici (DDoS, ransomware, data breach) → rischio per i dati e reputazione.
- Blackout o problemi di connettività → impossibilità di accesso ai servizi.
- Errori umani → perdita o alterazione involontaria di dati.

Obiettivi di ripristino

Servizio Critico	RTO (Tempo massimo di ripristino)	RPO (Perdita massima di dati)
Masternet Box	1 ora	30 minuti
Prenotabanca	1 ora	30 minuti
Viadiretto	1 ora	30 minuti
Vetrina DS	1 ora	5 minuti
Vetrina Light	1 ora	5 minuti

5. Strategie di Continuità Operativa

- Ridondanza multi-region: replica dei dati e failover manuale su cloud provider secondario. Il servizio è garantito dal fornitore tecnico (Aruba SPA) dove sono installati i sistemi tecnologici Master Chart. Il partner applica standard tier di livello 4 e ha, tra le altre, certificazioni ISO 22301-1, ISO 27001, ISO 27017, ISO 27018, ISO 27035, ISO 9001, ISO 14001, ISO 50001, CSA STAR Livello 2, ANSI/TIA-942, ISO 22237.
- Backup frequenti: backup quotidiani per i database, retention fino a cinque anni.

- Cybersecurity avanzata: firewall, monitoraggio continuo, mitigazione DDoS.
- Disaster Recovery Plan: ambiente di test per simulazioni e ripristino controllato.

6. Procedure di Attivazione

Quando si attiva il piano?

- Downtime critico superiore a 5 minuti.
- Violazione di sicurezza con impatto sui dati.
- Perdita di accesso ai servizi per cause esterne (es. disastro naturale).

Fasi di attivazione

1. Rilevazione → Monitoraggio automatico segnala l'anomalia.
2. Escalation → L'Incident Manager avvia il piano e informa i responsabili.
3. Mitigazione → Attivazione failover, ripristino dati, risposta a cyber attacchi.
4. Comunicazione → Email ai clienti e aggiornamenti interni.
5. Risoluzione e verifica → Test finali, revisione delle azioni intraprese.

7. Test ed Esercitazioni

Test	Frequenza	Obiettivo	Responsabile	KPI di Successo
Test di Backup e Ripristino	Semestrale	Verifica dell'integrità dei dati	IT Security Team	RTO < 4h, RPO < 1h
Failover Infrastruttura Cloud	Annuale	Test dello switch automatico tra region	Cloud Operations	RTO < 10 min
Simulazione Cyber Attack	Annuale	Valutazione della risposta agli attacchi	Security Team	Tempo di risposta < 30 min
Disaster Recovery Completo	Biennale	Simulazione di guasto totale	CIO, IT Ops	Ripristino < 8h
Continuità Operativa Team	Annuale	Verifica continuità operativa team di supporto e sviluppo	HR, IT Support	100% operatività da remoto

8. Manutenzione e Aggiornamento

- Revisione annuale del piano, con aggiornamento in base a nuove minacce o infrastrutture.
- Analisi post-evento: dopo ogni incidente, è stabilito che venga redatto un report con indicazione di eventuali miglioramenti da implementare.

Il presente documento è stato aggiornato nel mese di dicembre 2025.

MASTER CHART S.r.l.
Via Eugenio Montale, 2 - 25087 Salò (BS)
Tel. 0365 / 41778 r.a. Fax 0365 / 40378
C.C.I.A.A. 0345672 Trib. BS 52011
P. IVA e C.F. 01736620988
Indirizzo Internet www.masterchart.it
E-mail info@masterchart.it
Cap. Soc. Euro 100.000,00 i.v.