

ALLEGATO I – BUSINESS CONTINUITY PLAN (PIANO DI CONTINUITÀ OPERATIVA) – VERSIONE CONDIVISIBILE

REVISIONI	VERS.	DATA	DESCRIZIONE	AUTORE
	1	03/03/2023	Prima stesura	Roberto Martina
	2	30/07/2025	Seconda stesura	Roberto Martina
	3	17/02/2026	Terza stesura	Roberto Martina
	4	27/04/2026	Quarta stesura	Roberto Martina

VALIDATO DA	Roberto Martina	DATA 27/04/2026	FIRMA
APPROVATO DA	Roberto Martina	DATA 27/04/2026	FIRMA

INDICE

CONTROLLO DEL DOCUMENTO	4
1. DEFINIZIONI	5
2. FINALITÀ E AMBITO DI APPLICAZIONE	6
2.1. FINALITÀ	6
2.2. EVENTI CONSIDERATI	6
2.3. PERIMETRO DI APPLICAZIONE E LIMITAZIONI	6
2.4. TIMEFRAME COPERTO DAL PIANO	6
3. DESTINATARI	7
4. RIFERIMENTI	8
5. GOVERNANCE, RUOLI E RESPONSABILITÀ	9
5.1. RESPONSABILE CONTINUITÀ OPERATIVA (RCO)	9
5.2. COMITATO DI GESTIONE DELLA CRISI (CMT)	9
5.3. INCIDENT RESPONSE TEAM (IRT)	9
5.4. MATRICE DECISIONALE E RESPONSABILITÀ PER LIVELLO DI EMERGENZA	10
6. BUSINESS IMPACT ANALYSIS (BIA) E SERVIZI CRITICI	11
6.1. SINTESI ATTIVITÀ BIA	11
6.2. LIVELLI DI EMERGENZA	11
6.3. LIVELLI DI CRITICITÀ DEL SERVIZIO	11
6.4. IDENTIFICAZIONE DEI SERVIZI CRITICI	11
6.5. PERSONALE MINIMO E SOSTITUZIONI	11
7. DIPENDENZE E FORNITORI RILEVANTI	12
7.1. FORNITORI RILEVANTI	12
8. STRATEGIE DI CONTINUITÀ	13
8.1. CONTINUITÀ “PERSONE”	13
8.2. CONTINUITÀ “SEDI”	13
8.3. CONTINUITÀ “TECNOLOGIA”	13
9. CRITERI DI ATTIVAZIONE, ESCALATION E GESTIONE DELL’EMERGENZA	15

CLASSIFICAZIONE DOCUMENTO:**RISERVATO**

CodiceWeb Business Innovation – CF/PI: 03505120984

<https://www.cwbi.it>

Via Venezia, 92/b – 35131 Padova (PD)

info@cwbi.it**ISO/IEC 27001:2024****Nr. IT.25.0111.00.ISM**

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

9.1.	SCENARI DI CRISI	15
9.2.	TRIGGER DI ATTIVAZIONE E CRITERI DI DISATTIVAZIONE	15
9.3.	PROCESSO DI ESCALATION E ATTIVAZIONE WAR-ROOM	15
9.4.	TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI)	15
10.	COMUNICAZIONI IN EMERGENZA	16
10.1.	CANALI E DESTINATARI	16
10.2.	CONTENUTO MINIMO DEGLI AGGIORNAMENTI VERSO IL CLIENTE	16
10.3.	REGISTRO DI CRISI E CONSERVAZIONE EVIDENZE	16
11.	PIANI DI CONTINUITÀ OPERATIVA PER SCENARIO (SINTESI OPERATIVA)	17
11.1.	INDISPONIBILITÀ DELLA SEDE PRIMARIA	17
11.2.	INDISPONIBILITÀ CONNETTIVITÀ INTERNET	17
11.3.	INDISPONIBILITÀ SISTEMI INFORMATIVI	17
11.4.	INDISPONIBILITÀ FORNITORI CRITICI	18
11.5.	INDISPONIBILITÀ PERSONALE MINIMO	18
12.	TEST, FORMAZIONE, POST-INCIDENT REVIEW E MIGLIORAMENTO CONTINUO	19
12.1.	PIANO TEST ANNUALE E CASI DI RI-TEST	19
12.2.	EVIDENZE E REPORTING (TEST RECORD)	19
12.3.	FORMAZIONE E CONSAPEVOLEZZA	19
12.4.	POST-INCIDENT REVIEW E AGGIORNAMENTO DEL BCP	19
13.	GESTIONE E AGGIORNAMENTO DEL DOCUMENTO	20

CONTROLLO DEL DOCUMENTO

Scopo

Il presente Business Continuity Plan (BCP) definisce governance, strategie, risorse e procedure per garantire la continuità operativa di CWBI a fronte di eventi avversi, con focus sui servizi ICT e sulle funzioni aziendali critiche.

Destinazione

Documento predisposto, in forma condivisibile, per esigenze dei Clienti.

Principio di minimizzazione e riservatezza (versione condivisibile)

Questa versione è “sanitizzata”: NON include dettagli tecnici sensibili quali, a titolo esemplificativo, indirizzi IP, regole firewall, configurazioni di sicurezza, inventario completo degli asset, log completi.

Tali informazioni, se indispensabili, sono condivisibili esclusivamente in modalità controllata, tramite specifica documentazione, NDA o similari.

Documenti correlati

- Disaster Recovery Plan (DRP) di CWBI (fornito congiuntamente al presente documento).

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

1. DEFINIZIONI

RTO (Recovery Time Objective):

tempo massimo tollerabile tra incidente e ripristino del servizio.

RPO (Recovery Point Objective):

massima perdita dati tollerabile espressa come tempo dall'ultimo punto consistente disponibile.

BCP/PCO:

Piano di Continuità Operativa (presente documento).

DRP (Disaster Recovery Plan):

Piano di ripristino tecnico-operativo, attivato per eventi severi/disastrosi.

RCO:

Responsabile Continuità Operativa.

CMT:

Crisis Management Team (Comitato di Gestione della Crisi).

IRT:

Incident Response Team (Team di Risposta).

CLASSIFICAZIONE DOCUMENTO:

RISERVATO

CodiceWeb Business Innovation – CF/PI: 03505120984

<https://www.cwbi.it>

Via Venezia, 92/b – 35131 Padova (PD)

info@cwbi.it

ISO/IEC 27001:2024

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

2. FINALITÀ E AMBITO DI APPLICAZIONE

2.1. FINALITÀ

Il Piano ha l'obiettivo di garantire una risposta tempestiva e coerente a eventi che compromettano, o possano compromettere, la continuità dei servizi e delle funzioni critiche, minimizzando impatti verso clienti e partner e assicurando il rispetto degli obblighi contrattuali (SLA e requisiti di servizio).

Il Piano mira in particolare a:

- definire un framework di resilienza operativa (governance, escalation, decision making);
- assicurare una gestione di crisi strutturata, includendo comunicazioni interne ed esterne;
- rendere misurabile l'efficacia della continuità tramite obiettivi (RTO/RPO), test e miglioramento continuo.

Il presente Piano è altresì predisposto in coerenza con il Regolamento (UE) 2022/2554 (Digital Operational Resilience Act – DORA) e con le relative norme tecniche di regolamentazione, quale componente del framework di gestione del rischio ICT adottato da CWBI.

2.2. EVENTI CONSIDERATI

Il Piano copre, in modo non esaustivo:

- malfunzionamenti applicativi e/o infrastrutturali;
- indisponibilità prolungata di connettività e/o energia;
- attacchi cyber e/o corruzione dati;
- indisponibilità di sedi e/o indisponibilità di fornitori critici;
- indisponibilità del personale minimo.

2.3. PERIMETRO DI APPLICAZIONE E LIMITAZIONI

Il BCP si applica a servizi ICT, processi di supporto e funzioni critiche di CWBI necessari all'erogazione dei servizi al Cliente.

Limitazioni e confini:

- Se il servizio/ambiente è "hostato o gestito dal Cliente", CWBI copre esclusivamente le attività in carico a CWBI (supporto applicativo, attività di ripristino nei limiti degli accessi e responsabilità contrattuali).
- Per i servizi erogati su infrastruttura cloud esterna gestita da CWBI, la continuità operativa è disciplinata secondo il modello di responsabilità condivisa. CWBI è responsabile delle componenti applicative, della configurazione logica, dei backup applicativi e del ripristino dei dati nei limiti del proprio perimetro di controllo. L'infrastruttura sottostante resta in carico al provider cloud secondo i relativi SLA contrattuali.

2.4. TIMEFRAME COPERTO DAL PIANO

Questo BCP copre:

- continuità e ripristino nel breve periodo (prime 0–72 ore) e nella fase di stabilizzazione;
- continuità in modalità degradata e recovery esteso fino a 7 giorni.

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

3. DESTINATARI

Destinatari interni:

- CDA/Direzione CWBI
- RCO, CMT, IRT
- Funzioni coinvolte in continuità (IT/Delivery/Amministrazione)

Destinatari esterni:

- Clienti (versione condivisibile)
- Eventuali fornitori critici solo se necessario per attivazione del Piano e limitatamente alle informazioni strettamente pertinenti.

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

4. RIFERIMENTI

- ISO 22301:2019
- ISO/IEC 27031:2011
- Regolamento (UE) 2022/2554 (DORA)
- Regolamento delegato (UE) 2024/1774 (RTS su ICT risk management framework)
- Regolamento di esecuzione (UE) 2024/2956 (modelli standard del registro delle informazioni)

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

5. GOVERNANCE, RUOLI E RESPONSABILITÀ

5.1. RESPONSABILE CONTINUITÀ OPERATIVA (RCO)

Il RCO mantiene il Piano, coordina test e aggiornamenti e, in emergenza, valuta l'impatto e propone/attiva l'escalation.

Responsabilità in ordinario:

- mantenimento e aggiornamento BCP/DRP;
- pianificazione test e raccolta evidenze;
- formazione minima e sensibilizzazione dei ruoli coinvolti;
- valutazione impatti di cambiamenti organizzativi/tecnologici.

Responsabilità in emergenza:

- punto di contatto;
- triage, classificazione e proposta/attivazione BCP/DRP;
- convocazione CMT, coordinamento IRT e comunicazioni;
- coordinamento rientro e consuntivo.

Nome	Azienda	Ruolo	Contatto	Reperibilità
Martina Roberto	CWBI	Responsabile Tecnico	business-continuity@cwbi.it	24x7

5.2. COMITATO DI GESTIONE DELLA CRISI (CMT)

È l'organo di governo dell'emergenza per eventi rilevanti e decide su attivazione del Piano (livello disastroso), priorità e comunicazioni esterne.

Responsabilità:

- dichiarazione stato di crisi;
- priorità di ripristino e allocazione risorse;
- decisioni su attivazione DRP e rientro;
- supervisione comunicazioni verso Cliente e fornitori.

Nome	Azienda	Ruolo	Contatto	Reperibilità
Martina Roberto	CWBI	Responsabile Tecnico	business-continuity@cwbi.it	24x7
Martina Roberto	CWBI	Responsabile Amministrativo	amministrazione@cwbi.it	24x7

5.3. INCIDENT RESPONSE TEAM (IRT)

Il Team di risposta gestisce la componente tecnica-operativa dell'incidente e attua i runbook del DRP.

Responsabilità:

- analisi tecnica e contenimento;
- ripristino e stabilizzazione;
- attuazione workaround;
- raccolta evidenze tecniche e consuntivo.

CLASSIFICAZIONE DOCUMENTO:

RISERVATO

CodiceWeb Business Innovation – CF/PI: 03505120984

<https://www.cwbi.it>

Via Venezia, 92/b – 35131 Padova (PD)

info@cwbi.it

ISO/IEC 27001:2024

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

Nome	Azienda	Ruolo	Contatto	Reperibilità
Ambarusi J.	CWBI	Area Delivery	jerom.ambarusi@cwbi.it	24x7
Cerkezi E.	CWBI	Area Sviluppo	ensar.cerkezi@cwbi.it	24x7
Callegarin E.	CWBI	Area Sviluppo	enrico.callegarin@cwbi.it	24x7

5.4. MATRICE DECISIONALE E RESPONSABILITÀ PER LIVELLO DI EMERGENZA

Livello	Classe	Decisione/Owner principale	Note operative
1	Ordinario	Operatore/IT on duty	Gestione operativa, no attivazione BCP
2	Moderato	RCO	Escalation se rischio superamento RTO
3	Elevato	RCO	Attivazione BCP; update Cliente se impattato
4	Disastroso	CMT	Attivazione BCP+DRP; comunicazioni di crisi strutturate

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

6. BUSINESS IMPACT ANALYSIS (BIA) E SERVIZI CRITICI

6.1. SINTESI ATTIVITÀ BIA

Nel corso del 2022 CWBI ha svolto una BIA per identificare processi/servizi rilevanti, impatti da indisponibilità, dipendenze (incluse terze parti), obiettivi di ripristino e personale minimo.

La Business Impact Analysis è riesaminata almeno annualmente o in occasione di modifiche significative a infrastruttura, servizi o fornitori critici.

6.2. LIVELLI DI EMERGENZA

Livello	Classe	Descrizione
1	Ordinario	Incidente senza impatti significativi, risolvibile da chi lo rileva.
2	Moderato	Incidente che impatta servizi non critici, rischio limitato.
3	Elevato	Incidente che impatta servizi critici, rischio compromissione continuità.
4	Disastroso	Incidente che causa l'interruzione estesa dei servizi (> 1 giorno) o perdita/compromissione significativa che richiede attivazione DRP.

6.3. LIVELLI DI CRITICITÀ DEL SERVIZIO

Livello	Classe	Descrizione
1	Basso	Il servizio/attività non impatta la mission aziendale.
2	Medio	Il servizio/attività offre supporto al perseguimento della mission aziendale, in caso di prolungata inattività si potrebbero verificare impedimenti nella normale operatività.
3	Alto	Il servizio/attività è fondamentale per il perseguimento della mission aziendale e la sua compromissione danneggia gravemente o paralizza l'operatività aziendale.

6.4. IDENTIFICAZIONE DEI SERVIZI CRITICI

Servizio	Livello (Classe) Criticità	RTO	RPO	Referenti	Personale ordinario	Personale minimo
Sviluppo	3 (Alto)	8h	8h	Martina R.	20	5
Mail	2 (Medio)	24h	24h	Martina R.	1	1
Cloud	3 (Alto)	2h	24h	Martina R.	1	1

6.5. PERSONALE MINIMO E SOSTITUZIONI

La tabella seguente formalizza il presidio minimo e le sostituzioni, con personale già formato.

Servizio	Personale Minimo	Nominativi primari	Nominativi sostitutivi
Cloud	1	Martina R.	Zanon T.
E-mail	1	Martina R.	Zanon T.
Connettività Rete	1	Martina R.	Zanon T.
Sviluppo	5	Callegarin E., Cerkezi E.	Ambarusi J.

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

7. DIPENDENZE E FORNITORI RILEVANTI

7.1. FORNITORI RILEVANTI

Servizio/Asset	Descrizione	Fornitore	Impatto indicativo	Business Unit
E-mail	Server Posta	Aruba	critico dopo 4 ore	BUAA, BUAC, BUAT
Connettività	Connettività Internet	Vodafone	critico dopo 4 ore	BUAA, BUAC, BUAT
Server VPS	Server VPS	Aruba	critico dopo 4 ore	BUAA, BUAC, BUAT
Server VPS	Server VPS	AWS	critico dopo 4 ore	BUAA, BUAC, BUAT

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

8. STRATEGIE DI CONTINUITÀ

8.1. CONTINUITÀ “PERSONE”

CWBI garantisce la continuità operativa mediante l'identificazione di ruoli critici, la definizione del personale minimo necessario e l'attivazione di misure organizzative per assicurare la reperibilità e la sostituibilità delle risorse chiave. Il modello prevede:

- reperibilità dei ruoli di continuità e del team tecnico;
- possibilità di operare da remoto tramite accesso autenticato e canali cifrati
- piano di sostituzione del personale minimo per i servizi critici, con attività periodiche di rotazione e formazione per mantenere la capacità di subentro.

Il personale minimo e i sostituti sono definiti al paragrafo 6.5. In caso di indisponibilità di una o più risorse chiave, il RCO coordina l'attivazione delle sostituzioni e, se necessario, la riallocazione temporanea delle attività e delle priorità di ripristino, secondo i livelli di emergenza (par. 6.2) e gli obiettivi RTO/RPO applicabili.

8.2. CONTINUITÀ “SEDI”

CWBI adotta un modello di continuità basato su sedi fisiche alternative e sulla capacità di operare da remoto per i ruoli critici. La sede primaria è ubicata a Padova e la sede secondaria a Brescia. La sede secondaria è predisposta per ospitare il personale minimo e consentire le attività necessarie alla gestione degli incidenti, al ripristino e al presidio operativo dei servizi, secondo quanto previsto dal presente BCP e dal DRP.

Capacità e utilizzo:

- Sede primaria: Padova, via Venezia 92/b
- Sede secondaria: Brescia, via Montesuello 6/a
- Postazioni disponibili: Padova: 40 – Brescia: 5.

Condizioni di attivazione della sede secondaria:

- indisponibilità della sede primaria oltre le soglie definite ai paragrafi 11;
- eventi di sicurezza o incidenti che richiedano la segregazione operativa e/o attività di ripristino (secondo DRP);
- indisponibilità prolungata di servizi essenziali in sede primaria (energia, connettività), non risolvibile entro tempi compatibili con RTO/RPO applicabili.

Modalità operative in continuità:

- Attivazione del lavoro da remoto per il personale minimo tramite VPN e canali cifrati.
- Trasferimento presso la sede secondaria del personale minimo quando richiesto dalla durata/gravità dell'evento.
- Per i servizi del Cliente erogati su cloud esterno, la continuità della “sede” riguarda principalmente il presidio operativo (supporto, incident handling, ripristino logico) e non l'hosting fisico del servizio; la capacità di operare da remoto e dalla sede secondaria garantisce la prosecuzione delle attività.

8.3. CONTINUITÀ “TECNOLOGIA”

CWBI adotta misure tecniche e procedurali per garantire la disponibilità e la recuperabilità delle componenti ICT a supporto dei servizi erogati. Il modello di continuità tecnologica si basa su:

- capacità di ripristino su sito/ambiente alternativo;

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

- strategie di backup e replica coerenti con gli obiettivi RTO/RPO;
- procedure di ripristino formalizzate nel Disaster Recovery Plan (DRP);
- misure di accesso sicuro per l'operatività remota (autenticazione, canali cifrati).

Per i servizi del Cliente erogati su cloud esterno, la continuità tecnologica dipende anche dalle responsabilità condivise e dalle dipendenze da subfornitori. I dettagli operativi di ripristino (runbook, sequenze di restore, verifiche di integrità e procedure “safe restore” in caso di ransomware) sono disciplinati nel DRP.

CLASSIFICAZIONE DOCUMENTO:**CodiceWeb Business Innovation – CF/PI: 03505120984**

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024**RISERVATO**<https://www.cwbi.it>info@cwbi.it**Nr. IT.25.0111.00.ISM**

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

9. CRITERI DI ATTIVAZIONE, ESCALATION E GESTIONE DELL'EMERGENZA

9.1. SCENARI DI CRISI

Sono considerati i seguenti macro-scenari:

- **IPM:** Indisponibilità del personale minimo
- **IS:** indisponibilità sedi / servizi essenziali.
- **ISINFO:** indisponibilità sistemi informativi.
- **IFC:** Indisponibilità dei fornitori critici

9.2. TRIGGER DI ATTIVAZIONE E CRITERI DI DISATTIVAZIONE

Attivazione BCP:

- quando è previsto superamento dell'RTO di un servizio critico o deterioramento a livello non accettabile;
- quando un incidente cyber impatta disponibilità/integrità e richiede azioni di contenimento o restore;
- quando indisponibilità di sede o fornitore critico non è risolvibile con workaround in tempi compatibili.

Disattivazione BCP:

Il BCP si considera disattivabile quando:

- il servizio è stabilizzato e rientrato nei livelli ordinari (o in modalità degradata accettata dal Cliente);
- sono completate le verifiche minime di integrità e funzionamento;
- è completata la comunicazione di "rientro" verso gli stakeholder rilevanti;
- è stato avviato il processo di consuntivo (registro di crisi + azioni correttive).

9.3. PROCESSO DI ESCALATION E ATTIVAZIONE WAR-ROOM

- **Livelli 1–2:** gestione tramite incident management operativo; escalation al RCO se l'impatto cresce.
- **Livello 3:** attivazione BCP decisa dal RCO; war-room tecnica attivata; comunicazioni al Cliente se impattato.
- **Livello 4:** dichiarazione stato di crisi dal CMT; attivazione BCP e DRP; comunicazioni di crisi strutturate.

9.4. TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI)

Tempo (dal rilevamento)	Obiettivo	Responsabile
T+15 minuti	Triage e classificazione livello	IRT/RCO
T+30 minuti	Decisione attivazione BCP (se Livello ≥3)	RCO (o CMT se Liv.4)
T+60 minuti	Prima comunicazione al Cliente per Liv.3–4 (se impattato)	RCO/CMT
T+4 ore	Aggiornamenti periodici fino a stabilizzazione	RCO/CMT

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

10. COMUNICAZIONI IN EMERGENZA

10.1. CANALI E DESTINATARI

Interno:

- war-room (canale tecnico) + aggiornamenti alla Direzione e CMT.

Esterno:

- Mailbox dedicata: business-continuity@cwbi.it

10.2. CONTENUTO MINIMO DEGLI AGGIORNAMENTI VERSO IL CLIENTE

Ogni comunicazione di crisi verso il Cliente riporta almeno:

- impatto e servizi coinvolti;
- azioni in corso e workaround;
- prossima milestone/ETA o time-box del successivo aggiornamento, includendo, ove applicabile, indicazione del rischio su RTO/RPO.

10.3. REGISTRO DI CRISI E CONSERVAZIONE EVIDENZE

CWBI mantiene un “Registro di Crisi” (event log) prontamente accessibile in caso di attivazione del BCP/DRP, contenente:

- timeline (orari, decisioni, azioni chiave, comunicazioni inviate);
- evidenze essenziali e riferimenti ai ticket;
- esito e data/ora di stabilizzazione e chiusura.

CLASSIFICAZIONE DOCUMENTO:

RISERVATO

CodiceWeb Business Innovation – CF/PI: 03505120984

<https://www.cwbi.it>

Via Venezia, 92/b – 35131 Padova (PD)

info@cwbi.it

ISO/IEC 27001:2024

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

11. PIANI DI CONTINUITÀ OPERATIVA PER SCENARIO (SINTESI OPERATIVA)

Nota: le attività tecniche di dettaglio sono disciplinate nel DRP. Il presente capitolo definisce trigger, soglie operative e modalità di attivazione.

11.1. INDISPONIBILITÀ DELLA SEDE PRIMARIA

Trigger:

- Indisponibilità della sede primaria (Padova) per impossibilità di accesso, inagibilità o indisponibilità di servizi essenziali, ad esempio energia elettrica.
- Interruzione dell'energia elettrica superiore a 15 minuti.
- Evento che comprometta la capacità operativa in sede oltre soglia compatibile con RTO dei servizi critici.

Azione:

- Utilizzo dei gruppi di continuità (UPS) per consentire lo spegnimento controllato delle apparecchiature locali.
- Se indisponibilità > 15 minuti:
 - attivazione operatività in modalità remota per il personale minimo tramite VPN e canali cifrati;
 - verifica impatto su servizi e priorità di presidio.
- Se indisponibilità > 24 ore:
 - trasferimento del personale minimo presso la sede secondaria (Brescia);
 - mantenimento operatività restante personale in modalità remota;
 - attivazione eventuali procedure di ripristino previste nel DRP.

Per i servizi erogati su infrastruttura cloud esterna, l'indisponibilità della sede primaria non comporta necessariamente indisponibilità dell'infrastruttura di produzione; la continuità è garantita tramite operatività remota e/o attivazione sede secondaria.

11.2. INDISPONIBILITÀ CONNETTIVITÀ INTERNET

Trigger:

- Indisponibilità della connettività primaria.
- Degrado significativo della banda tale da compromettere il rispetto degli RTO applicabili.

Azione:

- Attivazione connettività di backup (es. 4/5G) ove disponibile.
- Escalation immediata al fornitore.
- Se indisponibilità prolungata:
 - operatività da remoto su sede secondaria o altre connessioni alternative;
 - aggiornamento Cliente se impattato.

11.3. INDISPONIBILITÀ SISTEMI INFORMATIVI

Trigger:

- Indisponibilità applicazioni o database critici.

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

- Sospetto compromissione integrità dati.
- Evento cyber che impatti disponibilità o integrità.

Azione:

- Attivazione immediata containment.
- Classificazione livello incidente.
- Valutazione attivazione DRP.
- Ripristino da backup consistente secondo priorità definite in BIA.
- Verifica integrità prima della rimessa in produzione.

In caso di evento cyber, il ripristino avviene privilegiando ambienti logicamente segregati per evitare reinfezione.

11.4. INDISPONIBILITÀ FORNITORI CRITICI

Trigger:

- Indisponibilità di provider cloud, hosting, connettività o altro fornitore rilevante.

Azione:

- Escalation formale al fornitore.
- Attivazione workaround ove possibile.
- Se non risolvibile entro tempi compatibili con RTO:
 - attivazione procedure di disaster recovery o soluzione alternativa prevista;
 - comunicazione strutturata al Cliente.

11.5. INDISPONIBILITÀ PERSONALE MINIMO

Trigger:

- Assenza simultanea di risorse chiave tale da compromettere presidio servizio.

Azione:

- Attivazione sostituzioni previste al par. 6.5.
- Riallocazione priorità operative.
- Se capacità ridotta oltre soglia:
 - attivazione modalità degradata;
 - comunicazione al Cliente dei limiti temporanei.

Per “modalità degradata” si intende l'erogazione del servizio con funzionalità ridotte o con SLA temporaneamente rimodulati, previa comunicazione e, ove previsto, accettazione del Cliente.

12. TEST, FORMAZIONE, POST-INCIDENT REVIEW E MIGLIORAMENTO CONTINUO

12.1. PIANO TEST ANNUALE E CASI DI RI-TEST

CWBI effettua almeno un test annuale dei piani di continuità e ripristino; ulteriori test sono eseguiti in caso di cambiamenti sostanziali (nuove infrastrutture, cambi di fornitore critico, cambi architetturali rilevanti).

Scenari minimi: indisponibilità sito primario, indisponibilità sistemi informativi, ransomware/corruzione dati, indisponibilità fornitore critico.

12.2. EVIDENZE E REPORTING (TEST RECORD)

CWBI conserva evidenze dei test per un periodo massimo di 6 mesi.

12.3. FORMAZIONE E CONSAPEVOLEZZA

Il personale coinvolto (RCO, CMT, IRT, sostituti) riceve formazione almeno annuale o al variare di processi/ruoli/fornitori.

12.4. POST-INCIDENT REVIEW E AGGIORNAMENTO DEL BCP

A seguito di incidenti maggiori o di test con esito non pienamente soddisfacente, CWBI effettua un consuntivo (post-incident review) per identificare cause, efficacia delle procedure e miglioramenti necessari, aggiornando BCP/DRP se necessario.

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

13. GESTIONE E AGGIORNAMENTO DEL DOCUMENTO

- Revisione almeno annuale.
- Verifica annuale: nomine ruoli, reperibilità, accessi essenziali, capacità di ripristino, coerenza fornitori/SLA.
- Aggiornamento urgente in caso di: variazioni personale chiave, fornitori o contratti, infrastruttura, software rilevanti, sedi o modalità operative, cambi SLA.

FINE DOCUMENTO

CLASSIFICAZIONE DOCUMENTO:

CodiceWeb Business Innovation – CF/PI: 03505120984

Via Venezia, 92/b – 35131 Padova (PD)

ISO/IEC 27001:2024

RISERVATO

<https://www.cwbi.it>

info@cwbi.it

Nr. IT.25.0111.00.ISM

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.