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

| REVISIONI | VERS. | DATA | DESCRIZIONE | AUTORE |
|---|---|---|---|---|
| | 2 | 30/07/2025 | Seconda stesura | Team Sicurezza & Compliance |
| | 3 | 17/02/2026 | Terza stesura | Team Sicurezza & Compliance |
| | 4 | 27/04/2026 | Quarta stesura | Team Sicurezza & Compliance |
| | 5 | 07/09/2026 | Quinta stesura | Team Sicurezza & Compliance |

| | | | |
|---|---|---|---|
| **VALIDATO DA** | Responsabile SGSI | **DATA** 07/09/2026 | **FIRMA** |
| **APPROVATO DA** | Direzione | **DATA** 07/09/2026 | **FIRMA** |


**CodiceWeb Business Innovation – CF/PI: 03505120984** https://www.cwbi.it
Via Venezia, 92/b – 35131 Padova (PD) info@cwbi.it

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

**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** 7

**3. DESTINATARI** 8

**4. RIFERIMENTI** 9

**5. GOVERNANCE, RUOLI E RESPONSABILITÀ** 10

**5.1. RESPONSABILE CONTINUITÀ OPERATIVA (RCO)** 10
**5.2. COMITATO DI GESTIONE DELLA CRISI (CMT)** 10
**5.3. INCIDENT RESPONSE TEAM (IRT)** 11
**5.4. MATRICE DECISIONALE E RESPONSABILITÀ PER LIVELLO DI EMERGENZA** 11

**6. BUSINESS IMPACT ANALYSIS (BIA) E SERVIZI CRITICI** 12

**6.1. SINTESI ATTIVITÀ BIA** 12
**6.2. LIVELLI DI EMERGENZA** 12
**6.3. LIVELLI DI CRITICITÀ DEL SERVIZIO** 12
**6.4. IDENTIFICAZIONE DEI SERVIZI CRITICI** 12
**6.5. PERSONALE MINIMO E SOSTITUZIONI** 13

**7. DIPENDENZE E FORNITORI RILEVANTI** 14

**7.1. FORNITORI RILEVANTI** 14

**8. STRATEGIE DI CONTINUITÀ** 15

**8.1. CONTINUITÀ "PERSONE"** 15
**8.2. CONTINUITÀ "SEDI"** 15
**8.3. CONTINUITÀ "TECNOLOGIA"** 15


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 17**

**9.1. SCENARI DI CRISI 17**
**9.2. TRIGGER DI ATTIVAZIONE E CRITERI DI DISATTIVAZIONE 17**
**9.3. PROCESSO DI ESCALATION E ATTIVAZIONE WAR-ROOM 17**
**9.4. TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI) 18**

**10. COMUNICAZIONI IN EMERGENZA 19**

**10.1. CANALI E DESTINATARI 19**
**10.2. CONTENUTO MINIMO DEGLI AGGIORNAMENTI VERSO IL CLIENTE 19**
**10.3. REGISTRO DI CRISI E CONSERVAZIONE EVIDENZE 19**

**11. PIANI DI CONTINUITÀ OPERATIVA PER SCENARIO (SINTESI OPERATIVA) 21**

**11.1. INDISPONIBILITÀ DELLA SEDE PRIMARIA 21**
**11.2. INDISPONIBILITÀ CONNETTIVITÀ INTERNET 21**
**11.3. INDISPONIBILITÀ SISTEMI INFORMATIVI 21**
**11.4. INDISPONIBILITÀ FORNITORI CRITICI 22**
**11.5. INDISPONIBILITÀ PERSONALE MINIMO 22**

**12. TEST, FORMAZIONE, POST-INCIDENT REVIEW E MIGLIORAMENTO CONTINUO 24**

**12.1. PIANO TEST ANNUALE E CASI DI RI-TEST 24**
**12.2. EVIDENZE E REPORTING (TEST RECORD) 24**
**12.3. FORMAZIONE E CONSAPEVOLEZZA 24**
**12.4. POST-INCIDENT REVIEW E AGGIORNAMENTO DEL BCP 24**

**13. GESTIONE E AGGIORNAMENTO DEL DOCUMENTO 25**


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

## CONTROLLO DEL DOCUMENTO

### Scopo

Il presente Business Continuity Plan (BCP) definisce governance, strategie, risorse e procedure per garantire la continuità operativa e la resilienza di CWBI a fronte di eventi avversi, con focus sulle piattaforme applicative erogate in modalità SaaS, sui servizi ICT e sulle funzioni aziendali critiche, nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato UNI CEI EN ISO/IEC 27001:2022.

### 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. Per ragioni di sicurezza operativa (OPSEC), prevenzione di attacchi di ingegneria sociale e tutela dei dati personali, nella presente versione condivisibile i nominativi delle singole persone fisiche, i contatti personali diretti e le ragioni sociali puntuali dei subfornitori tecnologici sono espressi tramite Ruoli Funzionali e Categorie di Fornitura Qualificate.

### Documenti correlati

- Politica Generale di Sicurezza delle Informazioni di CWBI;
- Piano di Risposta agli Incidenti di Sicurezza e Data Breach (Incident Response Plan - IRP) di CWBI;
- Disaster Recovery Plan (DRP) di CWBI (documento tecnico-operativo interno contenente i runbook di ripristino).


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 il verificarsi dell'incidente/interruzione e il ripristino del servizio (target ≤ 2 ore per i servizi SaaS critici).

**RPO (Recovery Point Objective):**
massima perdita di dati tollerabile espressa come intervallo temporale dall'ultimo punto di consistenza disponibile (garantita tramite replica ad alta affidabilità, Point-in-Time Recovery - PITR e backup immutabili).

**BCP/PCO:**
Piano di Continuità Operativa (presente documento), volto a governare la continuità dei processi critici e la gestione strategica della crisi.

**DRP (Disaster Recovery Plan):**
Piano di ripristino tecnico-operativo delle infrastrutture ICT e Cloud IaaS, attivato per garantire il rispetto dell'RTO in caso di eventi severi o disastrosi.

**IRP (Incident Response Plan):**
Piano di Risposta agli Incidenti di Sicurezza e Data Breach, che disciplina il ciclo di gestione degli incidenti cyber (rilevazione, triage, contenimento, preservazione forense, eradicazione, ripristino e notifiche).

**Safe Restore:**
procedura prescrittiva di ricostruzione e ripristino dei sistemi operativi e database a partire da immagini certificate (Golden Images CIS Benchmarks) e backup immutabili WORM verificati esenti da compromissione, eseguita in ambiente segregato prima della rimessa in produzione.

**RCO:**
Responsabile Continuità Operativa.

**CMT:**
Crisis Management Team (Comitato di Crisi), presieduto dall'Alta Direzione.

**IRT:**
Incident Response Team (Team di Risposta agli Incidenti), coordinato dal Responsabile SGSI / CISO in qualità di Incident Commander.


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 conformità allo standard UNI CEI EN ISO/IEC 27001:2022 (Certificato Nr. IT.25.0111.00.ISM, controlli A.5.29, A.5.30, A.8.13, A.8.14), a supporto della resilienza operativa digitale e della conformità contrattuale dei Clienti soggetti al Regolamento (UE) 2022/2554 (Digital Operational Resilience Act - DORA) e relative norme tecniche di regolamentazione, nonché ai requisiti di continuità operativa, gestione dei backup, ripristino e sicurezza della catena di approvvigionamento previsti dall'Art. 24, comma 2, lett. c) e d) del D.Lgs. 138/2024 (Recepimento Direttiva UE 2022/2555 - NIS2).

## 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. CWBI progetta, sviluppa ed eroga soluzioni applicative proprietarie in modalità SaaS (Software-as-a-Service) poggianti su infrastrutture Cloud IaaS qualificati con Data Center situati esclusivamente all'interno del territorio dell'Unione Europea (UE) e certificati ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e SOC 2.

Gli uffici aziendali di CWBI (sede operativa di Padova e sede legale/secondaria di Brescia) non ospitano server fisici di produzione, rack dedicati all'erogazione dei servizi SaaS né database contenenti dati di produzione o dati personali dei Clienti.

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 IaaS qualificata (con Data Center nell'Unione Europea), la continuità operativa è disciplinata secondo il Modello di Responsabilità Condivisa (SaaS su IaaS): il Provider IaaS presidia la sicurezza fisica, la continuità elettrica e antincendio, l'hardware e le dorsali di rete, mentre CWBI presidia i sistemi operativi virtuali, i database, gli applicativi SaaS, la crittografia, i backup (conformi alla regola 3-2-1 con immutabilità temporale WORM) e il disaster recovery logico/applicativo.


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

## 2.4. 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.


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:

- Alta Direzione CWBI (Amministratore Unico / Legale Rappresentante)
- RCO, CMT, IRT
- Funzioni coinvolte in continuità (IT & Cloud Operations / AdS, Team Sviluppo & DevSecOps, Customer Success, Referente Privacy)

Destinatari esterni:

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


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

- UNI CEI EN ISO/IEC 27001:2022 (Controlli A.5.29, A.5.30, A.8.13, A.8.14) e linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019
- ISO 22301:2019 e ISO/IEC 27031:2011
- Direttiva (UE) 2022/2555 (NIS2) e D.Lgs. 4 settembre 2024, n. 138 (in particolare Art. 24, comma 2, lett. c, d, l e Art. 25)
- Regolamento (UE) 2022/2554 (DORA), Regolamento delegato (UE) 2024/1774 (RTS su ICT risk management framework) e Regolamento di esecuzione (UE) 2024/2956
- Regolamento (UE) 2016/679 (GDPR - Artt. 28, 32, 33 e 34)


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, operando in stretto raccordo con il Responsabile del SGSI / CISO (Incident Commander) e con l'Alta Direzione.

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.

| Figura / Presidio | Azienda | Ruolo | Contatto | Reperibilità |
|---|---|---|---|---|
| Responsabile Continuità Operativa (RCO) | CWBI | Coordinamento Continuità / Presidio Tecnico | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 |

### 5.2. COMITATO DI CRISI (CMT)

Il Comitato della Crisi (CMT) è presieduto dall'Alta Direzione (Amministratore Unico / Legale Rappresentante) - che detiene l'autorità esclusiva di deliberare formalmente lo stato di crisi, l'attivazione del BCP/DRP e le spese straordinarie - e integra il Responsabile Continuità Operativa (RCO), il Responsabile del SGSI / CISO (Incident Commander) e, per i profili di competenza, il Referente Privacy Interno e il Referente Relazioni Clienti B2B (Customer Success).

Responsabilità:

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

| Figura / Presidio | Azienda | Ruolo | Contatto | Reperibilità |
|---|---|---|---|---|
| Alta Direzione (Legale Rappresentante) | CWBI | Direzione Strategica e Delibera Crisi | amministrazione@cwbi.it | 24x7 |
| Responsabile Continuità Operativa (RCO) | CWBI | Coordinamento Continuità | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 |
| Responsabile SGSI / CISO | CWBI | Incident Commander / Sicurezza | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 |


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

### 5.3. INCIDENT RESPONSE TEAM (IRT)

Il Team di Risposta agli Incidenti (IRT) è guidato dal Responsabile del SGSI / CISO (Incident Commander). Nel rispetto del principio di Segregation of Duties, le manovre dirette sull'ambiente Cloud IaaS di produzione (isolamento logico, acquisizione snapshot immutabili, Safe Restore ed esecuzione dei runbook del DRP) sono eseguite esclusivamente dagli Amministratori di Sistema / IT & Cloud Operations (coordinati dall'IT & Cloud Operations Lead), mentre il Team di Sviluppo Software e DevSecOps (coordinato dal DevSecOps & Sviluppo Lead) supporta l'analisi delle vulnerabilità applicative e lo sviluppo/collaudo di hotfix in ambiente segregato di Staging, senza privilegi di modifica diretta in produzione.

Responsabilità:

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

| Figura / Presidio | Azienda | Ruolo | Contatto | Reperibilità |
|---|---|---|---|---|
| Responsabile SGSI / CISO | CWBI | Incident Commander | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 (alerting automatico e reperibilità secondo SLA contrattuali) |
| IT & Cloud Operations Lead / AdS | CWBI | Squadra Tecnica Infrastruttura Cloud IaaS e DRP | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 (alerting automatico e reperibilità secondo SLA contrattuali) |
| DevSecOps & Sviluppo Lead | CWBI | Supporto Applicativo SaaS e Hotfix (Staging) | business-continuity@cwbi.it (recapiti diretti on-call forniti in sede contrattuale) | 24x7 (Su attivazione IRT / Escalation) |

### 5.4. MATRICE DECISIONALE E RESPONSABILITÀ PER LIVELLO DI EMERGENZA

| Livello | Classe | Decisione/Owner principale | Note operative |
|---|---|---|---|
| 1 (P4) | Ordinario / Basso | Operatore IT on duty / AdS | Gestione operativa di routine, nessuna attivazione BCP/DRP |
| 2 (P3) | Moderato / Medio | IT & Cloud Operations Lead / RCO | Gestione tramite incident management; escalation a CISO/RCO se l'impatto cresce |
| 3 (P2) | Elevato / Alto | Incident Commander (CISO) / RCO | Valutazione attivazione DRP (se rischio superamento RTO <= 2h) e pre-allerta BCP; notifica Cliente se impattato |
| 4 (P1) | Disastroso / Critico | Alta Direzione / CMT (su proposta CISO/RCO) | Attivazione formale DRP (rischio RTO <= 2h / disastro IaaS > 1h) e BCP (indisponibilità > 4h o multi-tenant); comunicazioni di crisi strutturate |


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

Nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) certificato UNI CEI EN ISO/IEC 27001:2022, CWBI conduce e aggiorna periodicamente la Business Impact Analysis (BIA) per identificare processi e servizi critici, impatti da indisponibilità, dipendenze dalla catena di fornitura ICT, obiettivi di ripristino (RTO/RPO) e presidio minimo necessario.

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 (P4) | Ordinario / Basso | Evento o anomalia minore senza impatti sull'erogazione dei servizi SaaS né compromissione di dati. |
| 2 (P3) | Moderato / Medio | Incidente che impatta ambienti non di produzione (sviluppo/staging) o servizi interni non critici, risolvibile tramite workaround. |
| 3 (P2) | Elevato / Alto | Incidente grave con impatto su singolo tenant/servizio critico o degrado prestazionale, che richiede contenimento immediato e valutazione preventiva di continuità. |
| 4 (P1) | Disastroso / Critico | Incidente critico o sistemico che causa l'interruzione dei servizi SaaS di produzione con rischio di superamento dell'RTO (<= 2 ore, trigger DRP) o indisponibilità estesa (> 4 ore o multi-tenant, trigger BCP), ovvero attacco ransomware/compromissione grave. |

### 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 | Referente | Presidio Ordinario | Presidio Minimo |
|---|---|---|---|---|---|---|
| Piattaforma SaaS di Produzione e Infrastruttura Cloud IaaS (Applicativi Core, API, DBMS) | 3 (Alto) | <= 2h | Sub-orario / pochi minuti (target ordinario HA/PITR); <= 24h (baseline catastrofica off-site)* | IT & Cloud Operations Lead | Team IT & Cloud Ops | Presidio minimo garantito con sostituti abilitati |
| Ambienti di Sviluppo Software e Pipeline CI/CD | 3 (Alto) | 8h | 24h | DevSecOps & Sviluppo Lead | Team Sviluppo & DevSecOps | Presidio minimo garantito con sostituti abilitati |
| Servizi di Posta | 2 (Medio) | 24h | 24h | Amministratore | Presidio IT | Presidio |


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

| | | | | | | |
|---|---|---|---|---|---|---|
| Elettronica e Collaborazione Aziendale | | | | di Sistema Senior incaricato | Interno | continuativo con ridondanza di ruolo |

** Nota: per la Piattaforma SaaS di Produzione il target RPO operativo architetturale ordinario è sub-orario / pochi minuti (HA + PITR); <= 24 ore è la baseline di salvaguardia nello scenario catastrofico di restore da backup giornaliero immutabile off-site. Gli SLA contrattuali specifici possono prevedere RPO più stringenti e prevalgono sulla presente baseline.*

### 6.5. PERSONALE MINIMO E SOSTITUZIONI

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

| Servizio | Personale Minimo | Ruolo Primario Designato | Ruolo Sostitutivo (Backup) |
|---|---|---|---|
| Piattaforma SaaS / Cloud IaaS | 1-2 | IT & Cloud Operations Lead | Amministratore di Sistema (AdS) Senior |
| Servizi E-mail e Directory | 1 | IT & Cloud Operations Lead | Amministratore di Sistema (AdS) Senior |
| Connettività e Rete | 1 | IT & Cloud Operations Lead | Amministratore di Sistema (AdS) Senior |
| Sviluppo Software e DevSecOps | 2 | DevSecOps & Sviluppo Lead | Senior Software Developer |


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 / Categoria Qualificata | Impatto Indicativo | Perimetro / Funzione Coinvolta |
|---|---|---|---|---|
| Infrastruttura Cloud IaaS Primaria e DR | Data Center Cloud IaaS (VM, Storage, DBMS, Rete virtuale) | Provider Cloud IaaS Qualificato UE (ISO 27001 / SOC 2) | Critico (RTO <= 2h; trigger DRP se outage > 1h) | Erogazione Piattaforme SaaS / Produzione |
| Storage Backup Secondario Off-Site | Repository Backup Immutabile (WORM) geograficamente separato | Provider Cloud Qualificato UE (ISO 27001 / SOC 2) | Critico per Disaster Recovery e Safe Restore | Erogazione Piattaforme SaaS / Produzione |
| Connettività Internet Sedi | Connettività Primaria Fibra e Backup 4G/5G | Operatori TLC Primari Qualificati | Moderato (mitigato da telelavoro / linea backup) | Sedi Operative e Presidio Tecnico |
| Posta Elettronica e Collaborazione | Servizi Email Cloud e Comunicazione | Provider Cloud Qualificato (con canale OOB alternativo) | Medio (RTO 24h; comunicazioni di crisi garantite da canali alternativi Out-of-Band) | Tutte le Funzioni Aziendali |


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 esclusivamente tramite postazioni di lavoro aziendali gestite (con espresso divieto di utilizzo di dispositivi personali non gestiti - divieto di BYOD), equipaggiate con protezione anti-malware ed EDR centralizzato, attraverso tunnel VPN cifrati (AES-256) e Autenticazione Forte a Più Fattori (MFA obbligatoria);
- 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 sulla disponibilità di sedi fisiche alternative e sulla capacità di operare da remoto per tutti i ruoli critici. La sede operativa primaria è ubicata a Padova e la sede secondaria a Brescia. La sede secondaria è predisposta per ospitare il personale minimo di emergenza 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 (PD), via Venezia 92/b
- Sede legale e secondaria di continuità: Brescia (BS), via Montesuello 6/a
- La sede secondaria è attrezzata per ospitare il presidio minimo operativo di emergenza.

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.
- Poiché nessun server fisico di produzione né database contenente dati dei Clienti o dati personali è ospitato presso le sedi di Padova o Brescia (essendo l'intera infrastruttura di produzione attestata su Data Center Cloud IaaS qualificati situati esclusivamente nell'Unione Europea), l'eventuale inagibilità fisica delle sedi aziendali non interrompe l'erogazione dei servizi SaaS ai Clienti, ma comporta unicamente l'attivazione immediata del lavoro da remoto sicuro (VPN + MFA) e/o il trasferimento del presidio minimo operativo sulla sede di continuità di Brescia.

## 8.3. CONTINUITÀ "TECNOLOGIA"


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

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:

- architettura Cloud IaaS ad Alta Affidabilità (HA) priva di Single Point of Failure (SPoF), con bilanciamento del carico, cluster database in replica continua e distribuzione su Data Center qualificati situati esclusivamente nell'Unione Europea (UE);
- strategia di backup conforme alla Regola 3-2-1 (almeno 3 copie dei dati su 2 supporti distinti e 1 copia off-site in Data Center secondario geograficamente separato nell'UE), con backup giornalieri e Point-in-Time Recovery (PITR) dei log transazionali;
- protezione dei backup mediante cifratura forte AES-256 (in transito e a riposo) e policy di immutabilità temporale WORM (Write Once, Read Many / Object Lock) a presidio contro attacchi ransomware;
- procedure prescrittive di Safe Restore (ricostruzione ex novo da Golden Images certificate CIS Benchmarks e ripristino dati da backup immutabili verificati in ambiente sandbox segregato) e regime di monitoraggio intensificato (Hyper-care per 72 ore) post-ripristino;
- misure di accesso amministrativo sicuro con autenticazione forte (MFA obbligatoria), tunnel VPN cifrati (AES-256) e procedura di emergenza tracciata (Break-Glass).

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.


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

**Trigger di Attivazione DRP (Disaster Recovery Plan):**

- Superamento o rischio di superamento dell'RTO: quando il tempo stimato per il contenimento e il ripristino ordinario supera o rischia seriamente di superare l'RTO ≤ 2 ore previsto per i servizi SaaS critici, l'Incident Commander / RCO propone formalmente all'Alta Direzione l'attivazione del DRP e ne coordina l'esecuzione tecnica;
- Disastro infrastrutturale del fornitore IaaS: in caso di disastro fisico o indisponibilità grave ed estesa dei Data Center del provider cloud o dei nodi primari di rete non risolvibile entro 1 ora, si attiva il DRP con failover su Data Center secondario geograficamente separato nell'UE per garantire il rispetto dell'RTO ≤ 2 ore;
- Attacco ransomware sistemico: in presenza di attacco ransomware sistemico che richieda la ricostruzione delle infrastrutture e il ripristino da backup immutabili off-site in ambiente segregato, si attiva il DRP.

**Trigger di Attivazione BCP e Comitato di Crisi (CMT):**
Indisponibilità estesa: quando l'indisponibilità supera le 4 ore o coinvolge più servizi critici o una pluralità di tenant, l'Alta Direzione attiva il BCP, convoca il Comitato di Crisi (CMT) e incarica il Responsabile Continuità Operativa (RCO) per la gestione strategica, le comunicazioni di crisi e l'allocazione delle risorse straordinarie;
Ransomware sistemico con impatto esteso: se l'attacco ransomware determina un'indisponibilità superiore a 4 ore o un impatto multi-tenant, all'attivazione tecnica del DRP si affianca l'attivazione strategica del BCP;
Indisponibilità prolungata di sede, connettività, fornitori critici o personale minimo: qualora l'evento non sia risolvibile con i normali workaround operativi e rischi di compromettere gli accordi di servizio.

**Criteri di Disattivazione BCP e Rientro:**

Il BCP e il DRP si considerano formalmente disattivabili quando:

- il servizio è stabilizzato e rientrato nei livelli ordinari (o in modalità degradata formalmente concordata con il Cliente);
- sono completate le verifiche di integrità dei dati, coerenza applicativa e sicurezza post-ripristino;
- è completata la comunicazione formale di "rientro" verso tutti gli stakeholder rilevanti (Clienti e Autorità);
- è stato formalmente avviato il processo di consuntivo (Registro di Crisi, Post-Incident Review e piano CAPA).

### 9.3. PROCESSO DI ESCALATION E ATTIVAZIONE WAR-ROOM

- Livelli 1-2 (Severity P4-P3): gestione ordinaria tramite incident management operativo da parte degli Amministratori di Sistema; escalation a CISO e RCO se l'impatto o la durata crescono;
- Livello 3 (Severity P2): valutazione immediata di attivazione DRP da parte dell'Incident Commander (CISO) e del RCO (qualora emerga rischio di superamento dell'RTO <= 2h), pre-allerta del BCP e attivazione della war-room tecnica; notifica formale tempestiva al Cliente se impattato;


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

- Livello 4 (Severity P1): convocazione straordinaria del Comitato di Crisi (CMT) e dichiarazione formale dello stato di crisi da parte dell'Alta Direzione (su proposta dell'Incident Commander / RCO); attivazione formale del DRP al verificarsi dei trigger tecnici di §9.2 (rischio superamento RTO ≤ 2h, outage IaaS > 1h o ransomware sistemico) e del BCP in caso di indisponibilità estesa (> 4h) o impatto multi-tenant/multi-servizio; comunicazioni di crisi strutturate verso Clienti, Autorità ed enti regolatori.

### 9.4. TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI)

| Finestra Operativa | Obiettivo | Responsabile |
|---|---|---|
| T+15 minuti (P1 / Liv. 4) / T+30 minuti (P2 / Liv. 3) | Presa in carico, Triage analitico, classificazione severità e convocazione IRT | Incident Commander (CISO) / IRT |
| Al verificarsi dei trigger tecnici di §9.2 (rischio superamento RTO ≤ 2h, outage IaaS > 1h o ransomware sistemico), previa conferma dell'incidente a esito del triage | Valutazione e decisione attivazione DRP (se rischio superamento RTO <= 2h) e pre-allerta/attivazione BCP | Incident Commander (CISO) / RCO / Alta Direzione (CMT) |
| Dalla conferma dell'incidente a esito del triage, tempestivamente e senza indebito ritardo, nel rispetto degli SLA contrattuali, accordi DORA e DPA (ex Art. 28 GDPR) | Prima notifica formale al Cliente impattato (nel rispetto degli SLA contrattuali, accordi DORA e DPA ex Art. 28 GDPR) | Incident Commander (CISO) / Referente Relazioni Clienti B2B / RCO |
| Ogni 4 ore (o a ogni svolta significativa) | Aggiornamenti periodici di avanzamento fino a completa stabilizzazione e chiusura | Incident Commander (CISO) / Referente Relazioni Clienti B2B / RCO |


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:

- **Attivazione della War Room tecnica e aggiornamenti continui all'Alta Direzione e al CMT**. Qualora i canali ordinari aziendali (es. posta elettronica o sistemi interni) risultino compromessi o indisponibili, vengono attivati immediatamente i Canali di Comunicazione Sicura Fuori Banda (Out-of-Band - OOB), costituiti da messaggistica cifrata end-to-end su piattaforma esterna indipendente, caselle email di emergenza su dominio esterno protette da MFA forte e War Room virtuale su tenant separato, in piena conformità al §3.3 dell'IRP e all'Art. 24, comma 2, lett. l) del D.Lgs. 138/2024 (NIS2).

Esterno:

- **Mailbox dedicata di presidio:** business-continuity@cwbi.it e canali contrattuali/PEC presidiati dal Referente Relazioni Clienti B2B (Customer Success) su delega e coordinamento dell'Incident Commander (CISO);
- **Notifiche verso i Clienti:** effettuate tempestivamente e senza indebito ritardo nel rispetto degli SLA contrattuali, accordi DORA e DPA (ex Art. 28 GDPR); per i Clienti del settore bancario e finanziario soggetti al Regolamento (UE) 2022/2554 (DORA), CWBI fornisce supporto tempestivo per consentire il rispetto dei termini di notifica verso le Autorità di Vigilanza competenti ex Art. 19 DORA;
- **Notifiche verso le Autorità (CSIRT Italia / ACN):** CWBI garantisce il supporto informativo immediato ai Clienti soggetti NIS2 (ex Art. 24, comma 2, lett. d) e assolve agli obblighi di notifica diretta al CSIRT Italia / ACN ex Art. 25 del D.Lgs. 138/2024 ove applicabile in ragione del perimetro soggettivo aziendale (ovvero a titolo di notifica volontaria ex Art. 26), tramite la piattaforma di segnalazione del CSIRT Italia secondo le tempistiche di legge (preallarme entro 24 ore, notifica formale entro 72 ore, relazione finale entro 1 mese).
- **Notifiche al Garante per la Protezione dei Dati Personali e ai Titolari:** in caso di violazione di dati personali (data breach), il Referente Privacy Interno (privacy@cwbi.it) coordina le notifiche di legge ai sensi degli Artt. 33 e 34 del GDPR entro 72 ore solo ove CWBI operi quale Titolare autonomo (dati interni); per i dati trattati sulle piattaforme SaaS quale Responsabile del Trattamento (ex Art. 28 GDPR), CWBI notifica tempestivamente il Cliente Titolare e lo supporta con le evidenze tecniche per l'eventuale notifica al Garante.

### 10.2. CONTENUTO MINIMO DEGLI AGGIORNAMENTI VERSO IL CLIENTE

Ogni comunicazione di crisi verso il Cliente riporta almeno:

- data e ora di rilevazione dell'incidente e natura generale dell'evento;
- sistemi, tenant, applicativi o servizi SaaS coinvolti e stima preliminare dell'impatto;
- misure di containment, strategie di ripristino e workaround già attuati o pianificati;
- tempo stimato di ripristino (ETA) o finestra temporale del successivo aggiornamento, con evidenza del rispetto dei parametri RTO e RPO;
- riferimenti del Single Point of Contact (SPOC) tecnico per le comunicazioni di crisi;
- a conclusione dell'emergenza, trasmissione del report conclusivo di incidente (Executive Incident Summary).

### 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.


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

**CodiceWeb Business Innovation – CF/PI: 03505120984** https://www.cwbi.it
Via Venezia, 92/b – 35131 Padova (PD) info@cwbi.it

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.


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 delle manovre di contenimento logico selettivo (isolamento VM, regole WAF/firewall, revoca credenziali/token IAM) da parte degli Amministratori di Sistema.
- Per incidenti gravi (P1/P2) o sospetto atto illecito, preventiva cristallizzazione forense delle evidenze (snapshot immutabili dei volumi IaaS, acquisizione RAM ove fattibile, congelamento log con hash SHA-256 e Catena di Custodia).
- Valutazione ed esecuzione del DRP (se rischio superamento RTO <= 2 ore) con failover su infrastruttura secondaria.
- Eradicazione della causa radice e ripristino tramite procedura prescrittiva di Safe Restore (ricostruzione ex novo delle macchine virtuali da Golden Images certificate CIS Benchmarks e ripristino dati da backup immutabili WORM e log transazionali PITR).
- Collaudo funzionale, verifica di consistenza del database e scansione di sicurezza in ambiente sandbox segregato prima della rimessa in produzione, seguiti da 72 ore di monitoraggio intensificato (Hyper-care).

In caso di evento cyber, il ripristino avviene mediante procedura di Safe Restore in ambiente di sandbox segregato, eseguendo la scansione approfondita delle immagini e la bonifica delle vulnerabilità prima della rimessa in produzione.

### 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:
  - in caso di disastro fisico o indisponibilità grave del Data Center IaaS primario non risolvibile entro 1 ora (compatibilmente con l'RTO ≤ 2 ore), attivazione immediata del DRP con failover sul Data Center secondario geograficamente separato nell'Unione Europea, restando altresì predisposta la Strategia di Uscita (Exit Strategy) per la portabilità di container e database;
  - 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.


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

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.


**CodiceWeb Business Innovation – CF/PI: 03505120984** https://www.cwbi.it
Via Venezia, 92/b – 35131 Padova (PD) info@cwbi.it

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

# 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 (in raccordo con il §7.2 dell'IRP e il §12.2 della Politica Generale); ulteriori test sono eseguiti in caso di cambiamenti sostanziali (nuove infrastrutture, cambi di fornitore critico, cambi architetturali rilevanti). Il programma annuale include sia esercitazioni strategiche sia test tecnici pratici (Tabletop Crisis Exercise e Restore Test / Technical Drill di Isolamento e Safe Restore da backup immutabili WORM in ambiente di collaudo isolato, con verifica della consistenza dei dati e dei tempi di ripristino rispetto agli obiettivi RTO/RPO).

Scenari minimi testati: indisponibilità del sito primario, indisponibilità prolungata dei sistemi informativi, attacco ransomware / corruzione logica dei dati, indisponibilità grave del provider Cloud IaaS.

## 12.2. EVIDENZE E REPORTING (TEST RECORD)

CWBI verbalizza formalmente gli esiti, i tempi di ripristino rilevati e le eventuali azioni di miglioramento di ciascun test e conserva i relativi report ed evidenze documentali (Test Record) per almeno 3 anni (intero ciclo di certificazione SGSI ISO/IEC 27001, o per periodi superiori ove previsto da requisiti normativi o contrattuali), a supporto degli audit interni, delle verifiche dell'Organismo di Certificazione e delle attività di Vendor Due Diligence dei Clienti.

## 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 (Livello 3-4 / P1-P2) l'Incident Commander e il RCO convocano il Post-Mortem Meeting entro 5 giorni lavorativi dalla stabilizzazione, elaborando il Post-Incident Report comprensivo di Root Cause Analysis (RCA) e piano di Azioni Correttive e Preventive (CAPA), aggiornando il Registro dei Rischi aziendale e procedendo alla revisione event-driven del BCP/DRP/IRP entro 15 giorni lavorativi dalla chiusura dell'incidente qualora emergano margini di miglioramento.


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**


**CodiceWeb Business Innovation – CF/PI: 03505120984** https://www.cwbi.it
Via Venezia, 92/b – 35131 Padova (PD) info@cwbi.it

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