

ALLEGATO L – DISASTER RECOVERY PLAN – VERSIONE CONDIVISIBILE

REVISIONI	VERS.	DATA	DESCRIZIONE	AUTORE
	1	03/03/2023	Prima stesura	Roberto Martina
	2	30/07/2025	Seconda stesura	Roberto Martina
	3	27/04/2026	Terza 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. RELAZIONE CON IL BCP	6
3. DESTINATARI	7
4. RIFERIMENTI	8
5. GOVERNANCE, RUOLI E RESPONSABILITÀ	9
5.1. RUOLI (COERENZA CON BCP)	9
5.2. REPERIBILITÀ E CONTATTI	9
5.3. MATRICE DECISIONALE PER LIVELLO DI EMERGENZA (ALLINEATA CON BCP)	9
6. COMPONENTI IN SCOPE E PRIORITÀ DI RIPRISTINO	10
6.1. PRINCIPIO DI PRIORITÀ E COERENZA CON BIA	10
6.2. OBIETTIVI DI RIPRISTINO (RTO/RPO)	10
7. STRATEGIA DI BACKUP, REPLICA E PROTEZIONE DEI BACKUP	11
7.1. PRINCIPI	11
7.2. OGGETTI DI BACKUP (ALTO LIVELLO)	11
7.3. FREQUENZE E RETENTION	11
7.4. VERIFICHE, TEST DI RIPRISTINO E LOGGING	11
8. STRATEGIA DI DISASTER RECOVERY (RECOVERY OPTIONS)	12
8.1. APPROCCIO GENERALE (ON-PREM / CLOUD ESTERNO)	12
8.2. SAFE RESTORE (RANSOMWARE / INTEGRITÀ DATI)	12
8.3. CREDENTIAL ROTATION (CREDENZIALI/TOKEN/CHIAVI)	12
9. CRITERI DI ATTIVAZIONE, ESCALATION E GESTIONE DELL'EMERGENZA	13
9.1. TRIGGER DI ATTIVAZIONE DRP	13

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.

9.2.	CRITERI DI DISATTIVAZIONE DRP	13
9.3.	PROCESSO DI ESCALATION E WAR-ROOM (ALLINEATO CON BCP)	13
9.4.	TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI)	13
10.	COMUNICAZIONI IN EMERGENZA E SUPPORTO AL CLIENTE	14
10.1.	OBBLIGHI DI NOTIFICA	14
10.2.	REGISTRO DI CRISI E CONSERVAZIONE EVIDENZE	14
11.	PROCEDURE DI DISASTER RECOVERY PER SCENARIO (SINTESI OPERATIVA)	15
11.1.	INCIDENTE CYBER / RANSOMWARE (SAFE RESTORE)	15
11.2.	CORRUZIONE / CANCELLAZIONE DATI	15
11.3.	INDISPONIBILITÀ CLOUD PROVIDER / AMBIENTE DI EROGAZIONE	15
11.4.	INDISPONIBILITÀ CAPACITÀ OPERATIVA (SEDI / FULL-REMOTE)	15
11.5.	INDISPONIBILITÀ CONNETTIVITÀ	16
11.6.	INDISPONIBILITÀ FORNITORI CRITICI	16
12.	TEST, EVIDENZE, VAPT, POST-INCIDENT REVIEW E MIGLIORAMENTO CONTINUO	17
12.1.	PIANO TEST ANNUALE E RI-TEST	17
12.2.	EVIDENZE E REPORTING	17
12.3.	VULNERABILITY ASSESSMENT / PENETRATION TEST	17
12.4.	POST-INCIDENT REVIEW E AGGIORNAMENTO DRP	17
13.	GESTIONE E AGGIORNAMENTO DEL DOCUMENTO	18

CONTROLLO DEL DOCUMENTO

Scopo

Il presente Disaster Recovery Plan (DRP) definisce le strategie e le procedure tecnico-operative per ripristinare, in modo sicuro e tracciabile, i servizi, le applicazioni e i dati necessari all'erogazione dei servizi ICT, a seguito di eventi "disaster" o incidenti ICT gravi. Il DRP è integrato e coerente con il Business Continuity Plan (BCP) di CWBI.

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, credenziali, inventario completo degli asset, log completi, runbook "comando-per-comando".

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

Documenti correlati

- Business Continuity Plan (BCP) 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 (documento di governance e gestione crisi).

DRP (Disaster Recovery Plan):

Piano di ripristino tecnico-operativo (presente documento).

Safe Restore:

ripristino da punto consistente verificato non compromesso, su ambiente segregato, con verifiche di integrità prima del rientro in esercizio.

War-room:

struttura operativa di coordinamento durante incidenti Livello 3–4.

Fornitori critici / Terze parti TIC:

soggetti la cui indisponibilità può compromettere RTO/RPO o la continuità del servizio.

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 DRP ha l'obiettivo di assicurare la capacità di ripristino dei servizi e dei dati entro parametri coerenti con il BCP e con gli SLA applicabili, minimizzando downtime e perdita dati e garantendo un ripristino "sicuro" in caso di incidente cyber. Il piano definisce anche i criteri di attivazione/disattivazione, le responsabilità, le comunicazioni e le evidenze da conservare.

2.2. EVENTI CONSIDERATI

Il DRP copre, in modo non esaustivo:

- incidenti cyber, compromissione o corruzione dati;
- indisponibilità dell'ambiente di erogazione;
- indisponibilità prolungata della capacità operativa (sedi, accesso, servizi essenziali);
- indisponibilità connettività o degradazione severa;
- indisponibilità fornitori critici e/o dipendenze di supply chain.

2.3. PERIMETRO DI APPLICAZIONE E LIMITAZIONI

Il DRP si applica alle componenti ICT necessarie al ripristino dei servizi in scope. La versione condivisibile non include dettagli tecnici sensibili; tali dettagli sono disponibili solo in modalità controllata.

Per servizi su infrastruttura cloud esterna, il DRP si applica alle componenti in carico a CWBI (applicazione, configurazioni logiche, backup applicativi, ripristino dati nel perimetro controllato) e coordina le attività dipendenti dal provider secondo SLA del provider e responsabilità condivise.

2.4. RELAZIONE CON IL BCP

- Il BCP governa escalation, decision making, comunicazioni di crisi, ritorno alla normalità e post-incident review.
- Il DRP governa le procedure tecnico-operative di ripristino (restore, failover/switchover se applicabile, safe restore).

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:

- RCO, CMT, IRT (ruoli definiti nel BCP)
- Funzioni coinvolte in ripristino e gestione incidenti (IT/Delivery)

Destinatari esterni:

- Clienti (versione condivisibile)
- Auditor/Autorità o terze parti incaricate, esclusivamente secondo contratti/NDA e modalità controllata

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. RUOLI (COERENZA CON BCP)

- RCO (BCP): coordina e, per Livello 3, può decidere l'attivazione delle misure di ripristino nel perimetro DRP; coordina comunicazioni e consuntivo.
- CMT (BCP): per Livello 4 decide dichiarazione crisi, priorità e attivazione completa DRP, inclusi eventuali ripristini straordinari.
- IRT (BCP): esegue le attività tecniche di contenimento e ripristino secondo DRP.

5.2. REPERIBILITÀ E CONTATTI

Mailbox dedicata: business-continuity@cwbi.it

5.3. MATRICE DECISIONALE PER LIVELLO DI EMERGENZA (ALLINEATA CON BCP)

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. COMPONENTI IN SCOPE E PRIORITÀ DI RIPRISTINO

6.1. PRINCIPIO DI PRIORITÀ E COERENZA CON BIA

Le priorità di ripristino seguono i risultati della BIA e la criticità del servizio (BCP cap. 6). In caso di incidente cyber, la priorità è garantire integrità e prevenire reinfezione, anche a costo di un ripristino più lento.

6.2. OBIETTIVI DI RIPRISTINO (RTO/RPO)

Gli obiettivi RTO/RPO e i prerequisiti sono definiti nel BCP. Il DRP si impegna a rispettare tali obiettivi nei limiti del perimetro controllabile e dei prerequisiti dichiarati.

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. STRATEGIA DI BACKUP, REPLICA E PROTEZIONE DEI BACKUP

7.1. PRINCIPI

- 3-2-1: almeno tre copie, su almeno due “logiche” differenti, con almeno una copia offsite/segregata.
- Segregazione e safe restore: in cyber, ripristino su ambiente segregato prima del rientro in esercizio.
- Immutabilità/anti-manomissione: backup critici protetti da cancellazione/manomissione da account operativi standard.
- Cifratura in transito e a riposo e controllo accessi basato su ruoli.

7.2. OGGETTI DI BACKUP (ALTO LIVELLO)

- Database applicativi: PostgreSQL.
- File e repository applicativi (sorgenti/artefatti di rilascio) nei limiti del perimetro.
- Configurazioni applicative e parametri necessari al ripristino (escludendo segreti in chiaro; segreti gestiti tramite KMS).

7.3. FREQUENZE E RETENTION

- Backup database: cadenza giornaliera.
- Backup file/archivi: cadenza giornaliera.
- Replica verso capacità secondaria: giornaliera.

7.4. VERIFICHE, TEST DI RIPRISTINO E LOGGING

- Ogni test o attivazione DRP produce evidenze minime: esito, tempi misurati vs RTO/RPO, gap e remediation.
- Logging delle operazioni di backup e replica conservato con accesso controllato e retention coerente con policy (BCP - 10.3/12).

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. STRATEGIA DI DISASTER RECOVERY (RECOVERY OPTIONS)

8.1. APPROCCIO GENERALE (ON-PREM / CLOUD ESTERNO)

- Servizi corporate/on-prem: ripristino tramite capacità alternativa (sede secondaria o ambiente alternativo) secondo DRP.
- Servizi Cliente su cloud esterno: ripristino basato su procedure applicative/DB nel perimetro CWBI e coordinamento con provider per eventi infrastrutturali; applicazione di workaround o modalità degradata se necessario.

8.2. SAFE RESTORE (RANSOMWARE / INTEGRITÀ DATI)

In caso di sospetta compromissione:

- contenimento immediato e stop propagazione;
- identificazione ultimo recovery point consistente pre-evento;
- ripristino su ambiente segregato;
- verifiche minime (integrità dati + check funzionali minimi);
- rientro controllato in esercizio.

8.3. CREDENTIAL ROTATION (CREDENZIALI/TOKEN/CHIAVI)

In caso di incidente cyber o sospetto compromesso:

- invalidazione sessioni/token e disabilitazione account sospetti;
- rotazione credenziali privilegiate e segreti applicativi;
- verifica accessi post-rotazione e logging.

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

9.1. TRIGGER DI ATTIVAZIONE DRP

Il DRP si attiva quando:

- incidente Livello 3–4 con impatto su disponibilità/integrità e rischio superamento RTO/RPO;
- ransomware/cyber incident con necessità di safe restore;
- indisponibilità dell'ambiente di erogazione o del cloud provider senza workaround entro soglie compatibili;
- corruzione/cancellazione dati critici.

9.2. CRITERI DI DISATTIVAZIONE DRP

Il DRP si considera disattivabile quando:

- servizio stabilizzato (ordinario o degradato accettato dal Cliente);
- verifiche minime completate;
- comunicazione di chiusura inviata;
- avvio post-incident review e remediation.

9.3. PROCESSO DI ESCALATION E WAR-ROOM (ALLINEATO CON BCP)

- Livelli 1–2: gestione ordinaria; escalation al RCO se l'impatto cresce.
- Livello 3: war-room tecnica attiva; attivazione DRP nel perimetro necessario; comunicazioni al Cliente se impattato.
- Livello 4: dichiarazione crisi da CMT; attivazione completa DRP; comunicazioni strutturate e tracciamento completo.

9.4. TEMPI VERIFICABILI DI RISPOSTA (SLA DI CRISI)

Target operativi (allineati con BCP):

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 E SUPPORTO AL CLIENTE

10.1. OBBLIGHI DI NOTIFICA

CWBI comunica per iscritto al Cliente il verificarsi di Incidenti Operativi o di Sicurezza entro e non oltre 12 ore dalla rilevazione, includendo azioni svolte e/o azioni richieste al Cliente, per consentire l'attivazione delle procedure di gestione/emergenza nelle rispettive competenze.

10.2. REGISTRO DI CRISI E CONSERVAZIONE EVIDENZE

CWBI mantiene un Registro di Crisi contenente:

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

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.

11. PROCEDURE DI DISASTER RECOVERY PER SCENARIO (SINTESI OPERATIVA)

Nota: le attività tecniche di dettaglio (runbook) sono disponibili internamente e condivisibili solo in modalità controllata.

11.1. INCIDENTE CYBER / RANSOMWARE (SAFE RESTORE)

Trigger:

- indicatori di compromissione, cifratura, accessi anomali, corruzione dati.

Azione:

- containment immediato; preservazione evidenze minime;
- selezione recovery point consistente pre-evento;
- restore su ambiente segregato;
- verifiche integrità e test funzionali minimi;
- credential rotation (se applicabile);
- rientro controllato in esercizio e stabilizzazione.

11.2. CORRUZIONE / CANCELLAZIONE DATI

Trigger:

- inconsistenze DB, cancellazioni accidentali/massive, errori di integrità.

Azione:

- stop propagazione; blocco job/repliche che amplificano la corruzione;
- restore selettivo o full da backup consistente;
- verifiche integrità; ripartenza per priorità.

11.3. INDISPONIBILITÀ CLOUD PROVIDER / AMBIENTE DI EROGAZIONE

Trigger:

- outage o degrado severo su cloud provider o ambiente di erogazione.

Azione:

- escalation al provider e attivazione workaround/mode degradato;
- se previsto contrattualmente: valutazione failover/switchover e gate Cliente;
- comunicazioni periodiche al Cliente fino a stabilizzazione.

11.4. INDISPONIBILITÀ CAPACITÀ OPERATIVA (SEDI / FULL-REMOTE)

Trigger:

- indisponibilità sedi, impossibilità accesso, assenza servizi essenziali > soglie.

Azione:

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.

- attivazione operatività full-remote per personale minimo (VPN/MFA);
- se necessario: trasferimento personale minimo su sede secondaria;
- mantenimento accesso ad ambienti cloud esterni e strumenti operativi;
- ripristino per priorità secondo BIA.

11.5. INDISPONIBILITÀ CONNETTIVITÀ

Trigger:

- indisponibilità connettività primaria o degrado severo.

Azione:

- attivazione fallback (es. 4/5G) ove disponibile;
- operatività da remoto su alternative;
- escalation immediata fornitore.

11.6. INDISPONIBILITÀ FORNITORI CRITICI

Trigger:

- indisponibilità fornitori critici (hosting, connettività, DNS, monitoring, ecc.).

Azione:

- escalation formale al fornitore e attivazione workaround;
- se non risolvibile entro soglie compatibili con RTO: attivazione opzioni alternative (ove disponibili) e comunicazione strutturata al Cliente;

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.

12. TEST, EVIDENZE, VAPT, POST-INCIDENT REVIEW E MIGLIORAMENTO CONTINUO

12.1. PIANO TEST ANNUALE E RI-TEST

CWBI effettua almeno un test annuale delle capacità di ripristino e ulteriori test in caso di cambiamenti sostanziali o incidenti Livello 3–4. Scenari minimi: safe restore ransomware, restore DB, outage cloud provider, corruzione dati, perdita capacità operativa.

12.2. EVIDENZE E REPORTING

CWBI conserva test record completi (interni) e può condividere verso il Cliente un test summary sanitizzato contenente: data/scenario, esito, tempi misurati (RTO/RPO), principali gap e remediation plan (senza dettagli sensibili). Se richiesto, evidenze estese sono rese disponibili in data-room/audit.

12.3. VULNERABILITY ASSESSMENT / PENETRATION TEST

CWBI condivide con cadenza annuale i risultati di vulnerability assessment e penetration test, evidenziando vulnerabilità e proposta di remediation (tempi e modalità). In presenza di vulnerabilità critiche/alte emerse durante test, CWBI comunica tempestivamente al Cliente.

12.4. POST-INCIDENT REVIEW E AGGIORNAMENTO DRP

A seguito di incidenti Livello 3–4 o test con esito non pienamente soddisfacente, CWBI esegue PIR, aggiorna DRP/BCP se necessario e traccia le azioni correttive fino a chiusura.

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 o event-driven (cambio fornitore critico, variazioni architetturali, modifiche policy backup, esiti test/incidenti).
- Aggiornamento urgente in caso di: variazioni supply chain, data location, subfornitura (richiede autorizzazione preventiva Cliente se applicabile), cambi SLA o requisiti contrattuali.

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.