Cerved

Cerved Group S.p.A

Policy di Continuità Operativa

TIPO DI DOCUMENTO: POLICY	
Redazione	BCM Coordinator
Verifica	Task Force BCM

REVISIONI

N° REV.	DATA REV.	NOTE
001	30.03.2011	Prima emissione
002	30.03.2012	Revisione periodica
003	28.03.2013	Revisione periodica
004	28.03.2014	Revisione periodica
005	30.03.2015	Revisione periodica
006	30.03.2016	Revisione periodica
007	30.03.2017	Revisione periodica
008	30.03.2018	Revisione periodica
009	20.05.2021	Revisione periodica
010	01.09.2021	Aggiornamento modello organizzativo
011	31.01.2022	Revisione periodica
012	31.01.2023	Revisione periodica
013	12.12.2023	Revisione periodica

Approvata dal Comitato direttivo per la Gestione delle Emergenze

in data 12 dicembre 2023

INDICE

1 Scopo e campo di applicazione 4
2 Riferimenti e standard 5
3 Obiettivi della Continuità Operativa 7
4 Perimetro di riferimento per la Continuità Operativa 9
5 Leadership e committment 10
6 Il processo di gestione della Continuità Operativa 12
6.1 Analisi del contesto e Business Impact Analysis 13
6.2 Risk Assessment 14
6.3 Aggiornamento del framework documentale della Continuità Operativa 15
6.3.1 Piano di Continuità Operativa 15
6.3.2 Piano di Disaster Recovery 17
6.3.3 Procedure di contingenza 17
6.4 Test del Piano di Continuità Operativa 18
6.5 Formazione ed awareness 19
6.6 Misurazione, monitoraggio e miglioramento continuo 20
7 Allegati 22
7.1 Glossario 22

1 Scopo e campo di applicazione

La gestione della Continuità Operativa (o *Business Continuity, BC*) ha assunto una rilevanza fondamentale per tutte quelle Società che, per la tipologia del proprio contesto di business, devono garantire alti livelli di servizio ai propri clienti.

Questa necessità nasce sia per esigenze cogenti (es. normative di settore, clausole contrattuali, etc.), sia per una maggiore consapevolezza (valutazione del rischio) degli impatti sul business aziendale a seguito di eventuali eventi disastrosi.

Il Gruppo Cerved (di seguito "Cerved") impiega una varietà di personale, sia interno che esterno, applicazioni e sistemi informatici/informativi che prendono parte ad una serie complessa di processi interconnessi per garantire i servizi ai clienti. In questo contesto la gestione della continuità operativa aziendale mira a garantire la disponibilità di processi aziendali critici, anche nel caso di una emergenza.

L'obiettivo di questo documento è definire le politiche aziendali per la definizione del Piano di Continuità Operativa di Cerved e del Gruppo CCMG (PCO, di seguito anche BCP, *Business Continuity Plan*), in termini di principi, linee guida e regole per lo sviluppo, il mantenimento e l'esercizio dei Piani di Continuità Operativa in conformità allo Standard UNI EN ISO 22301:2019 e ai requisiti aziendali.

In particolare, il documento:

- individua gli obiettivi, i ruoli e le responsabilità necessari per lo sviluppo, l'esercizio e il mantenimento del Piano di Continuità Operativa di Cerved e Piano di Continuità Operativa del Gruppo CCMG;
- stabilisce i principi atti a garantire gli interventi di emergenza e ripristinare le operazioni e le attività di business.

I sistemi informativi sono utilizzati in modo pervasivo in tutti i processi aziendali. Essendo una risorsa fondamentale, necessitano di un programma di gestione della continuità aziendale (BCM) appropriato.

Quanto definito nel presente documento deve essere applicato per l'intero insieme di strutture organizzative e tecnologiche di tutte le Società che costituiscono il Gruppo Cerved.

2 Riferimenti e standard

Lo sviluppo dei piani di Continuità Operativa è fortemente condizionato da una serie di obblighi normativi nazionali italiani ed internazionali, cui si aggiungono specifiche normative di settore e standard di riferimento (norme ISO).

Per la definizione del seguente Piano di Continuità Operativa sono stati rispettati i seguenti standard e prescrizioni normative:

- *ISO 22301:2019*: lo Standard UNI EN ISO 22301:2019 – *Societal security – Business continuity management systems – Requirements* è lo standard internazionale di riferimento per la Business Continuity e Disaster Recovery. Fornisce alle organizzazioni un framework per pianificare, stabilire, attuare, gestire, monitorare, verificare, mantenere e migliorare continuamente il BCMS;
- *ISO 27001:2017:* lo Standard UNI CEI ISO/IEC 27001:2017 (*Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti*) è una norma internazionale – di cui Cerved Group ha conseguito certificazione - che definisce i requisiti per definire e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System) in merito ad aspetti di sicurezza logica, fisica ed organizzativa. In particolare, nell'Annex A "*Control objectives and controls*" sono specificati dei "controlli" per la gestione della Continuità Operativa a cui, l'azienda che intende applicare la norma, deve attenersi;
- *Regolamento UE 2016/679 – GDPR*: il regolamento generale sulla protezione dei dati (GDPR) prevede nell'Art.32 la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e che permettano, tra le altre, di ripristinare tempestivamente la disponibilità e l'accesso dai dati personali in caso di incidente fisico o tecnico.
- *ISO 22313:2020 - Societal security - Business continuity management systems - Guidance, ISO*: fornisce linee guida basate su best practices internazionali per la pianificazione, la creazione, l'implementazione, il funzionamento, il monitoraggio, la revisione, la manutenzione e il miglioramento continuo di un sistema di gestione documentato che consente alle organizzazioni di prepararsi, rispondere e riprendersi da eventi distruttivi.
- *ISO 22317:2019 - Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA), ISO;* fornisce una guida per un'organizzazione per stabilire, implementare e mantenere un processo di Business Impact Analysis (BIA) formale e documentato. Questa specifica tecnica non prescrive un processo uniforme per l'esecuzione di un BIA, ma aiuterà un'organizzazione a progettare un processo BIA appropriato alle sue esigenze.

- *ISO/IEC 27031:2011 - Information Technology - Security techniques - Guidelines for information and communication technology readiness for business continuity, ISO*: descrive i concetti e i principi della preparazione delle tecnologie dell'informazione e della comunicazione (ICT) per la continuità aziendale e fornisce un quadro di metodi e processi per identificare e specificare tutti gli aspetti (come criteri di prestazione, progettazione e implementazione) per migliorare la preparazione ICT di un'organizzazione per garantire la continuità aziendale. Si applica a qualsiasi organizzazione (privata, governativa e non governativa, indipendentemente dalle dimensioni). L'ambito di ISO / IEC 27031: 2011 comprende tutti gli eventi e gli incidenti (inclusi quelli relativi alla sicurezza) che potrebbero avere un impatto sull'infrastruttura e sui sistemi ICT.
- *ISO/IEC 27035-1:2016 - Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management, ISO:* presenta i concetti e le principali fasi per la gestione degli incidenti di sicurezza delle informazioni e combina questi concetti con i principi in un approccio strutturato per rilevare, segnalare, valutare e rispondere agli incidenti e applicare le lezioni apprese.
- *ISO 31000:2018 Risk management – Guidelines, ISO:* fornisce principi, framework, indicazioni metodologiche ed un processo per la gestione del rischio.

3 Obiettivi della Continuità Operativa

La Continuità Operativa – intesa come la capacità di una organizzazione di erogare i propri prodotti o servizi ad un livello accettabile prestabilito a seguito di eventi che ne causino l'interruzione (ISO 22300:2018) - deve essere integrata nei processi aziendali.

Questo obiettivo è soddisfatto mediante l'adozione di un Sistema di Gestione della Continuità Operativa (SGCO) che si propone di:

- assicurare un'adeguata formazione, informazione e sensibilizzazione sui requisiti del Sistema di Gestione della Continuità Operativa delle persone che lavorano nell'ambito di applicazione dello stesso, al fine di aumentarne la consapevolezza;
- incoraggiare le persone a segnalare gli eventi critici, nonché le osservazioni su come migliorare il SGCO;
- istituire e mantenere un processo strutturato per l'identificazione e la valutazione del rischio, con lo scopo di applicare gli opportuni controlli atti alla riduzione del livello di rischio identificato;
- stabilire, attuare e mantenere un processo di valutazione formale e documentata di Business Impact Analysis (BIA) per stabilire i processi e le attività più critiche ed il loro tempo di ripristino, mediante la definizione degli indicatori di continuità operativa tra cui: Recovery Time Objective (RTO), Recovery Point Objective (RPO), Maximum Tolerable Period of Disruption (MTPD) and the Minimum Business Continuity Objective (MBCO);
- elaborare e mantenere aggiornati dei Piani di Continuità Operativa e contingenza contenenti misure (organizzative, tecniche, operative) e procedure necessarie per garantire la disponibilità dei servizi, locali e persone anche in situazioni di crisi;
- definire, implementare, monitorare e migliorare continuamente un processo di incident response, incluso un modello organizzativo ed operativo, che permetta di rispondere in modo efficace agli incidenti;
- definire una formulazione di obiettivi misurabili e piani di miglioramento continuo ed una valutazione costante dei loro risultati;
- esercitare e testare le proprie procedure di Continuità Operativa per assicurare che siano coerenti con i propri obiettivi di Continuità Operativa;
- assicurare che tutte le terze parti coinvolte nel SGCO siano adeguatamente gestite, monitorate e istruite tramite opportuna formalizzazione contrattuale;

- assicurare verifiche, ispezioni ed audit periodici atti ad identificare e prevenire eventuali situazioni di non conformità rispetto ai requisiti del sistema di gestione BC, alle policy/procedure di Gruppo ed alla normativa vigente;
- riesaminare periodicamente i risultati del SGCO con il Top Management per la revisione degli stessi e per assicurare il miglioramento continuo.

4 Perimetro di riferimento per la Continuità Operativa

L‘attuazione di un Sistema di Gestione presuppone la definizione del perimetro della Continuità Operativa, in termini di:

- individuazione dei processi critici, che dovranno essere necessariamente ripristinati in caso di una emergenza, in base ai livelli di servizio predefiniti;
- identificazione delle sedi primarie in cui vengono eseguiti i processi critici;
- identificazione delle risorse indispensabili per garantire la continuità dei processi critici (sia risorse interne che terze parti eventualmente coinvolte);
- identificazione dell’infrastruttura tecnologica indispensabile in caso di emergenza;
- identificazione dei rischi che possono impattare le diverse sedi e i possibili scenari di emergenza che devono essere mitigati con opportune strategie per il ripristino dei servizi minimi;
- individuazione di una specifica struttura organizzativa coinvolta nella gestione della Continuità Operativa.

5 Leadership e committment

Il Top Management del Gruppo Cerved crede fermamente nel valore e nell'importanza della continuità operativa e pertanto sostiene pienamente l'implementazione e lo sviluppo del SGCO mediante:

- l'efficace ed efficiente applicazione del Sistema di Gestione della continuità operativa implementato;
- l'identificazione dei principali ruoli in merito alla continuità operativa all'interno delle funzioni/BU/LE istituendo un modello organizzativo specifico per la gestione e l'implementazione della Business Continuity in azienda, nonché specifici ruoli e comitati per la gestione straordinaria di emergenze e crisi;
- la definizione e diffusione del documento di Policy di Continuità Operativa, da cui derivano le strategie di azione, linee guida e obiettivi di Business Continuity;
- lo sviluppo e il continuo aggiornamento di piani, istruzioni e processi al fine di gestire emergenze e crisi in modo tempestivo;
- la creazione di un quadro documentale contenente i piani predefiniti che descrivono in dettaglio come l'organizzazione gestisce un evento dannoso e come garantisce la continuità delle sue attività in caso di un evento disastroso;
- la regolare pianificazione di test ed esercitazioni di Business Continuity e Disaster Recovery;
- la comprensione dell'azienda attraverso l'identificazione dei suoi servizi chiave e delle attività critiche, nonché delle risorse necessarie al loro mantenimento, attraverso l'esecuzione e lo svolgimento delle attività di Business Impact Analysis e Risk Assessment;
- la revisione sistematica dell'intero SGCO per garantire la sua conformità e adeguatezza in relazione ai cambiamenti normativi, organizzativi, strategici e cambiamenti legislativi;
- la presentazione del Piano di Continuità Operativa al Comitato di Sicurezza;
- la definizione di programmi formativi in ambito Business Continuity;
- il perseguimento degli obiettivi individuate;
- la condivisione con tutto il personale delle informazioni relative agli aggiornamenti e l'evoluzione dei processi aziendali;
- la partecipazione al Riesame della Direzione.

Il Gruppo Cerved ha definito un Modello Organizzativo per la gestione della Continuità Operativa identificando specifici ruoli e responsabilità all'interno dell'organizzazione stessa per affrontare problematiche di tipo organizzativo (Business Continuity) e tecnologiche (Disaster Recovery).

È stato istituito un Comitato di Sicurezza (definito come Comitato Direttivo per la gestione delle emergenze in condizioni di crisi) che si occupa della gestione, coordinamento e sviluppo delle tematiche relative alla continuità operativa.

I Direttori e i responsabili di tutte le aree organizzative in perimetro sono responsabili della promozione e diffusione della cultura della gestione della continuità operativa in azienda.

L'eccellenza nell'erogazione dei propri servizi e la soddisfazione del cliente si ottengono garantendo l'efficienza e l'affidabilità dei servizi erogati attraverso il sistema dei processi aziendali, e anche attraverso l'adozione di soluzioni di Security e Business Continuity sviluppate in conformità con le best practice del settore.

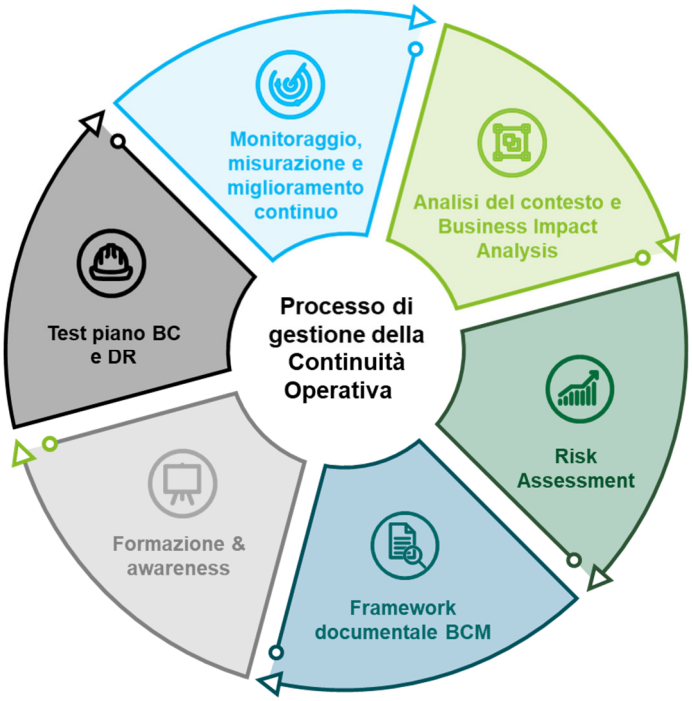
6 Il processo di gestione della Continuità Operativa

Il processo di Gestione della Continuità operativa in condizione ordinaria è coordinato dal BCM Coordinator e ha come obiettivo la manutenzione e il miglioramento continuo del Sistema di Gestione della Continuità operativa.

Il framework di continuità operativa del Gruppo si compone dei seguenti elementi fondamentali:

- Analisi del contesto e Business Impact Analysis
- Risk Assessment
- Framework documentale BCM (Piano di Continuità Operativa, Piano Disaster Recovery..)
- Formazione e awareness in ambito Continuità operativa
- Test piano BC e DR
- Monitoraggio, misurazione e miglioramento continuo

Nell'immagine che segue sono riportati i principali step del processo in condizione ordinaria:



6.1 Analisi del contesto e Business Impact Analysis

Obiettivi Analisi del contesto

Per assicurare il successo del Sistema di Gestione della Continuità Operativa, devono essere analizzate le parti interessate al fine di:

- coinvolgere ogni risorsa interessata al sistema di gestione implementato;
- semplificare la comunicazione con ognuno di essi, migliorare la comprensione della logica di business;
- ridurre i rischi che minacciano il raggiungimento dei benefici progettuali attesi.

Il dettaglio degli stakeholder, delle esigenze ad essi correlate, l'analisi del livello di influenza e le relative azioni correlate, devono essere dettagliati all'interno del documento di contesto.

Il requisito principale espresso da tutte le parti interessate è quello di possedere un sistema olistico composto da processi, risorse ed asset per garantire la disponibilità e l'integrità dei servizi offerti e gestiti dal Gruppo Cerved.

Obiettivi Business Impact Analysis

La Business Impact Analysis (BIA) rappresenta una delle attività chiave all'interno del Sistema di Gestione della Continuità Operativa ed ha come obiettivo la definizione, attuazione e manutenzione degli obiettivi e delle priorità in termini di continuità operativa e ripristino dei processi.

Le attività della Business Impact Analysis sono pertanto finalizzate alla raccolta di informazioni volte ad identificare e descrivere le aree di business più critiche o a rilevanza sistemica, dettagliando le risorse, umane, tecnologiche e logistiche, a supporto. Si tratta di una valutazione degli impatti sul business (economico-finanziari, legali, d'immagine-reputazionali e sul personale), determinati dal verificarsi di scenari di crisi che colpiscono risorse/asset di supporto ai processi aziendali, provocando l'indisponibilità delle relative attività e/o servizi.

La Business Impact Analysis, svolta dal Responsabile del processo, ha l'obiettivo di individuare, per ciascuna attività:

- le caratteristiche fondamentali (tipologia, criticità, impatti, ecc.);
- il massimo tempo di fermo sostenibile per l'attività (MTPD Maximum Tolerable Period of Disruption), ovvero il tempo entro il quale la stessa deve essere ripristinata ad un livello di servizio

predefinito. Tale attività consente di individuare, in accordo con gli indirizzi strategici e con le regole stabilite nel Piano di Continuità Operativa, il Tempo di Ripristino del processo (RTO);

- i requisiti e gli asset necessari a garantirne l'operatività in caso di emergenza, al fine di definire le soluzioni da implementare in funzione dei diversi livelli di criticità emersi e dello scenario di crisi verificatosi.

Metodologia

L'approccio utilizzato per la realizzazione della BIA deve essere un approccio Risk Based, ovvero un approccio basato sul rischio che comporta l'adozione di una visione globale dei rischi dell'attività aziendale e coinvolge l'alta direzione nell'intero processo di mitigazione dei rischi.

L'attività di BIA viene condotta con l'obiettivo di individuare RTO, RPO, MBCO e MTPD, nonchè gli impatti legati ad un disservizio e il subset minimo di risorse necessarie a garantire l'erogazione del processo di business.

L'attività di BIA deve essere preceduta da una fase di censimento di tutti i processi aziendali da sottoporre alla valutazione d'impatto del fermo del processo.

Il risultato della Business Impact Analysis rappresenta quindi il set informativo necessario per lo sviluppo delle soluzioni di continuità operativa.

6.2 Risk Assessment

Obiettivi

Le attività di Risk Assessment (RA) sono condotte per supportare il processo di identificazione, analisi e valutazione dei rischi, per determinare e tracciare le minacce che vengono gestite nel Piano di Continuità Operativa.

Metodologia

Il Risk Management è un approccio sistematico all'identificazione, valutazione, gestione e monitoraggio dei rischi. Il Gruppo Cerved, per svolgere le attività di analisi dei rischi inerenti la continuità operativa, si ispira alla ISO 31000.

La metodologia di valutazione del Rischio valuta in maniera distinta, la dimensione dell'impatto dalla dimensione della probabilità di accadimento.

L'analisi di impatto individua il livello di rischio relativo ai singoli processi aziendali e evidenzia le conseguenze della interruzione del servizio. L'allocazione delle risorse e le priorità di intervento sono correlate al livello di rischio.

6.3 Aggiornamento del framework documentale della Continuità Operativa

Obiettivi

Gli obiettivi principali che un sistema documentale di Business Continuity Management (BCM) deve consentire di perseguire, sono:

- la capacità di gestire l'insieme delle attività in maniera appropriata;
- essere attuale e efficace, consentendo, in caso di evento disastroso, la gestione della crisi e la ripartenza dei processi critici.

Uno degli aspetti più importanti del Sistema di Gestione della Continuità Operativa Management è la gestione della documentazione che deve essere:

- semplice e facile da comprendere;
- conforme rispetto ai requisiti di carattere normativo;
- fruibile, anche in situazioni di emergenza;
- efficace, riuscendo a fornire supporto manageriale, operativo e alle attività di controllo.

Tra i principali documenti in ambito Business Continuity si citano i seguenti:

6.3.1 Piano di Continuità Operativa

Obiettivi

I principali obiettivi del Piano di Continuità Operativa risultano essere i seguenti:

- fornire una guida da utilizzare durante una situazione di crisi del Gruppo Cerved al fine di rispondere in modo efficace e coerente a una situazione di crisi;

- documentare la fase di preparazione al fine di garantire che il Gruppo Cerved sia pronta a gestire una situazione di crisi (prontezza).

Principali contenuti

Il Piano di Continuità Operativa deve contenere i seguenti contenuti minimi:

- Processo di Continuità Operativa in condizioni ordinarie
- Organizzazione Continuità Operativa (ruoli e responsabilità in materia di Continuità Operativa)
- Scenari di crisi e strategie di contingenza
- Processo di Continuità Operativa in condizioni di emergenza/crisi

Con particolare riferimento agli scenari di crisi, il Piano di Continuità Operativa deve tenere in considerazione almeno i seguenti scenari:

- *Indisponibilità del top management***:** impossibilità di figure chiave del top management di essere presenti nelle sedi di lavoro e di essere comunque raggiungibili e operativi da remoto, per eventi quali pandemia, sciopero, ec
- *Indisponibilità del personale operativo essenziale***:** impossibilità di un elevato numero di figure chiave di essere presenti nelle sedi di lavoro e di essere comunque raggiungibili e operativi da remoto, per eventi quali pandemia, sciopero, ecc.
- *Indisponibilità di locali/sedi aziendali primarie, causa inaccessibilità***:** impossibilità di usufruire dei locali di una sede aziendale primaria, in quanto inagibile (es. incendio, terremoto o altro evento distruttivo) o irraggiungibile (es. allagamento o altro evento che impedisce di accedervi).
- *Interruzione funzionamento delle infrastrutture - energia elettrica***:** ipotesi di black-out prolungato che potrebbe compromettere il funzionamento delle postazioni di lavoro
- *Indisponibilità dei Sistemi IT***:** impossibilità di disporre dei sistemi IT utilizzati durante l'operatività ordinaria
- *Indisponibilità di apparecchiature informatiche (postazioni di lavoro):* indisponibilità delle postazioni di lavoro e/o delle attrezzature informatiche necessarie per il corretto svolgimento dell'operatività ordinaria.
- *Indisponibilità di documentazione cartacea e/o digitale***:** perdita o inaccessibilità a documenti cartacei e/o disponibili solamente in formato digitale indispensabili per garantire la Continuità Operativa;
- *Indisponibilità di fornitori (servizi e prodotti):* impossibilità da parte dei fornitori abituali e critici per il business aziendale di erogare i propri servizi/prodotti.

6.3.2 Piano di Disaster Recovery

Obiettivi

Il Disaster Recovery rappresenta l'insieme delle misure tecnologiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze.

Il Piano di DR si propone di garantire:

- la consapevolezza aziendale sulle tematiche di continuità e ripristino dei sistemi informativi;
- la preparazione delle azioni necessarie al recupero in caso di emergenza attraverso:
- lo sviluppo della capacità di gestire gli incidenti, le anomalie, le emergenze o le crisi, anche a fronte di eventuali modifiche organizzative;
- lo sviluppo di un insieme completo di misure (ad esempio procedure operative) per facilitare il ripristino dei servizi informatici e le attività di supporto a livelli di servizio predeterminati;
- l'assegnazione e il riconoscimento dei ruoli e delle responsabilità in caso di Disaster Recovery, tramite l'individuazione di adeguate risorse per una risposta efficace alle situazioni di emergenza o crisi, oltre a quelle essenziali per il business.

Principali contenuti

Il Piano di Disaster Recovery deve contenere i seguenti contenuti minimi:

- Perimetro di applicazione del Disaster Recovery
- Processo di gestione del Disaster Recovery in condizioni ordinarie
- Processo di attivazione del Disaster Recovery in condizioni di emergenza/crisi
- Organizzazione per il Disaster Recovery

6.3.3 Procedure di contingenza

Obiettivi

Le procedure operative di contingenza hanno l'obiettivo di declinare le attività che devono svolgere i ruoli previsti dal Modello Organizzativo per la Continuità Operativa al verificarsi di un evento di emergenza o crisi. Le procedure operative descrivono pertanto gli step operativi da seguire per garantire la continuità operativa.

Rientrano nelle procedure di contingenza ad esempio le seguenti:

- Procedura Disaster Recovery: contiene l'insieme di misure tecnologiche e il processo di attivazione del Disaster Recovery
- Procedure di contingenza processi critici: contiene l'insieme delle attività che i team dei processi critici dovranno eseguire per la riattivazione dei processi
- Procedura di comunicazione: contiene l'insieme delle attività che ciascun membro del Team di Comunicazione deve eseguire al verificarsi di un evento di emergenza o crisi. Le comunicazioni assumono un'importanza strategica nella gestione della continuità operativa. Una comunicazione corretta e strutturata verso l'esterno e verso l'interno consente di contrastare efficacemente possibili ripercussioni negative sull'immagine e sulla reputazione aziendale e facilita, al contempo, la pronta attivazione dei piani di emergenza elaborati.

Principali contenuti

Le procedure di contingenza devono contenere i seguenti contenuti minimi:

- Perimetro di applicazione della procedura
- Ruoli e responsabilità per la gestione delle emergenze
- Step operativi da seguire per la gestione delle emergenze

6.4 Test del Piano di Continuità Operativa

Obiettivi

L'attività di test si prefigge i seguenti obiettivi:

- identificare il grado di preparazione dell'azienda nel rispondere e gestire una situazione di crisi, come specificato nella strategia;
- valutare l'adeguatezza e il corretto aggiornamento del Piano di Continuità Operativa e/o del Piano di Disaster Recovery e delle procedure operative di dettaglio nel supportare il ripristino dell'operatività di business e informatica;
- valutare la preparazione dei team di gestione della Continuità Operativa e l'efficacia del programma di formazione;
- identificare le eventuali misure correttive/di miglioramento tali da comportare un aggiornamento del Piano di BC/DR o delle procedure operative.

Metodologia

Le metodologie di esercizio utilizzabili prevedono vari livelli di esercitazione, in base alla complessità dell'esercitazione stessa e all'obiettivo che si vuole raggiungere.

Come previsto dallo standard ISO 22301, i test e le esercitazioni sono parte fondamentale del SGCO e devono essere pianificati e svolti almeno annualmente al fine di verificare l'adeguatezza dei piani di continuità e di gestione di crisi.

Il programma di test deve essere variabile e flessibile tenendo in considerazione i cambiamenti organizzativi e gli esiti dei precedenti test.

I test devono essere articolati nelle seguenti fasi:

- Preparazione del test:
  - definizione dello scenario di emergenza da testare;
  - individuazione degli obiettivi;
  - definizione dei criteri di successo;
  - individuazione dei partecipanti al test;
  - definizione delle modalità di test (virtuale o live, parziale o totale).
- Esecuzione del test: esecuzione delle attività previste e pianificate secondo quanto stabilito nel piano di test.
- Verifica dei risultati del test: comprendere l'accaduto per individuare eventuali azioni preventive/correttive laddove siano stati rilevati margini di miglioramento;
- Predisposizione reportistica.

6.5 Formazione ed awareness

Obiettivi

Per la definizione, l'implementazione, la manutenzione e il miglioramento continuo del Sistema di Gestione della Continuità Operativa è necessario integrare la continuità operativa nella cultura aziendale, consentendogli di divenire parte dei valori chiave dell'organizzazione, accrescendo al tempo stesso la fiducia degli stakeholder circa la capacità della Società di far fronte ai fermi nell'operatività e alle situazioni di emergenza.

Il successo nello sviluppo e nell'implementazione del Sistema di Gestione della Continuità Operativa, in un contesto organizzativo caratterizzato da elementi culturali eterogenei, dipende dalla capacità di

integrazione di componenti quali, ad esempio, l'awareness e la formazione nella gestione strategica ed operativa dell'azienda, oltre che nelle priorità del business.

Lo sviluppo di una cultura della continuità operativa può essere conseguito attraverso:

- la definizione delle responsabilità;
- la formazione di competenze sia specifiche che generali in ambito di Continuità Operativa;
- L'integrazione degli elementi culturali legati alla continuità operativa permette al Gruppo Cerved di:
- sviluppare/attuare il Sistema di Gestione della Continuità Operativa in maniera più efficiente;
- infondere maggiore fiducia in generale negli stakeholders circa la capacità di gestire eventi di crisi/emergenze;
- assicurare che le implicazioni e gli aspetti correlati a tematiche di Continuità Operativa siano presi in considerazione a tutti i livelli aziendali.

Metodologia

Il processo di integrazione del Business Continuity Management all'interno della cultura aziendale è, generalmente, un'iterazione regolare delle seguenti tre attività:

- valutazione dell'attuale livello di consapevolezza e commitment sul BCM rispetto al livello desiderato, in modo tale da identificare lo scostamento esistente in termini di training/interventi mirati;
- progettazione e rilascio di contenuti formativi finalizzati a creare/rafforzare il livello di consapevolezza aziendale sulle tematiche in oggetto, sviluppando gli skill, le conoscenze e il commitment richiesti per una gestione efficace della continuità operativa;
- verifica del raggiungimento dei risultati programmati, monitorando il livello di Business Continuity awareness nel medio-lungo termine

6.6 Misurazione, monitoraggio e miglioramento continuo

Il Sistema di Gestione della Continuità Operativa deve essere costantemente sviluppato, misurato e migliorato.

Le attività necessarie sono:

- adattamento in base ai cambiamenti di natura tecnica ed organizzativa;
- estensione del campo di applicazione a parti organizzative aggiuntive e segmenti di business;

- adeguamento delle linee guida in funzione, ad esempio, di modifica degli standard;
- review di processo;
- ottimizzazione dei controlli di continuità operativa e riduzione dei rischi residui;
- eliminazione delle carenze, in particolare quelle che sono identificate in seguito ad audit o che possono portare a minacce concrete come reati.

L'approccio alla Continuità Operativa e il piano di Continuità Operativa devono essere regolarmente controllati mediante audit che hanno lo scopo di:

- garantire che il contenuto della politica, delle linee guida e delle policy/procedure sia noto e applicato;
- garantire che gli aspetti rilevanti nei processi della continuità operativa siano implementati e seguiti.

Infine, per garantire il miglioramento continuo del Sistema e di valutarne oggettivamente le prestazioni, occorre individuare, definire e monitorare periodicamente degli indicatori di prestazione (KPI).

7 Allegati

7.1 Glossario

TERMINE	DESCRIZIONE
Evento critico	Situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici o a rilevanza sistemica in seguito a incidenti o catastrofi.
Continuità Operativa (CO) /Business Continuity (BC)	Per Business Continuity si intende la capacità di continuare ad esercitare il proprio business a fronte di eventi catastrofici che possono colpirla. La Business Continuity si pone come obiettivo la continuità del servizio, per le applicazioni più critiche, o più raramente per l'intero landscape applicativo, entro un numero predeterminato di minuti/ore curando anche gli aspetti logistici e di fruizione dell'infrastruttura IT. Un progetto di BC comprende sempre anche un piano di DR.
Disaster Recovery (DR)	Per Disaster Recovery (brevemente DR) si intende l'insieme di misure tecnologiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze. Il Disaster Recovery si pone come obiettivo il ripristino di uno o più servizi IT entro un numero predeterminato di minuti/ore/giorni
Recovery Point Objetive (RPO)	L'RPO è uno dei parametri usati nell'ambito delle politiche di Disaster Recovery per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso. Al diminuire dell'RPO richiesto si rendono necessarie politiche di sicurezza sempre più stringenti e dispendiose, che possono andare dal salvataggio dei dati su supporti ridondanti tolleranti ai guasti fino alla loro pressoché immediata replicazione su un sistema informatico secondario d'emergenza (soluzione in grado di garantire, in linea teorica, valori di RPO prossimi allo zero).
Recovery Time Objective (RTO)	L'RTO è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo in un sistema di analisi Business Critical System (ad esempio implementazioni di politiche di Disaster Recovery nei Sistemi Informativi). È in pratica la massima durata, prevista o tollerata, del downtime occorso.
Scenario	Un set predefinito di eventi e condizioni che descrivono una interruzione, rottura o perdita relativa ad alcuni aspetti del business di una società, finalizzato all'esercizio del Piano di Continuità Operativa e del piano di Disaster Recovery e per definire le persone che dovranno gestire le attività in caso di emergenza.


Cerved