

**PIANO DI CONTINUITÀ OPERATIVA**

**(BUSINESS CONTINUITY PLAN)**

**Approvato dal Consiglio di Amministrazione**

Matrice delle revisioni

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  **Ed** | **Data** | **Rev** | **Data** | **Descrizione** | **Emesso da** | **Approvato da** |
| **00** | **29.04.2020** | **00** | **29.04.2020** | **Prima Emissione** | **Ufficio IT** | **CDA** |
| **00** | **29.04.2020** | **01** | **30.07.2021** | **revisione generica** | **Ufficio Organizzazione e IT** | **CDA** |

**Indice**

[1. Premessa e scopo 4](#_Toc104194943)

[2. Business Impact assessment 6](#_Toc104194944)

[3. Gestione dell’emergenza in fase di crisi o disastro 7](#_Toc104194945)

[4. Valutazione evento ed escalation 7](#_Toc104194946)

[4.1 Operazioni in caso di scenario no building 8](#_Toc104194947)

[4.2 Operazioni in caso di scenario no technology 10](#_Toc104194948)

[4.3 Operazioni in caso di scenario no people 10](#_Toc104194949)

[5. Attività connesse 11](#_Toc104194950)

# Premessa e scopo

Il presente documento descrive le attività da intraprendere in caso di criticità legate alla continuità operativa, che possono interessare ConfeserFidi; il documento formalizza i principi, fissa gli obiettivi e individua le procedure per la gestione della continuità operativa dei processi aziendali. Il documento si riferisce a tutti gli asset localizzati “on premises” che impattano soprattutto sull’attività commerciale.

Per quanto riguarda l’attività critica sottoposta alla vigilanza di Banca d’Italia, la continuità operativa è curata dalla società Galileo Network fornitore del software Parsifal, la quale trasmette al Confidi, a cadenza annuale, sia l’estratto dell’esito dei test effettuati di continuità operativa, sia i documenti relativi all’organizzazione degli stessi.

Può essere rilevante in questa sede quindi indicare che i dati relativi alla Vigilanza sono completamente esternalizzati e fruiti in SAAS (software as a service).

Sinteticamente l’attività connessa all’utilizzo di Parsifal è elencata di seguito:

* Antiriciclaggio e Archivio Unico Informatico, Segnalazione S.AR.A.
* Contrasto al Terrorismo e analisi delle operazioni sospette,
* Segnalazione in Centrale dei Rischi e di Vigilanza;
* Contabilità generale e Bilancio.
* Segnalazione dei rapporti continuativi e dei saldi
* Segnalazione apporto quote sociali

Inoltre, attraverso Parsifal vengono gestite le procedure di:

* Anagrafe generale
* Gestione degli accounts, dei livelli di accesso e della scadenza delle passwords
* Gestione dei dati finanziari ed economici dei soci o dei clienti
* Delibera, erogazione del credito di firma e per cassa
* Strumenti di mitigazione del rischio (es. FdG)
* Monitoraggio e dubbi esiti
* Contenzioso
* Reportistica
* Stampa delibere e contratti

Nel Manuale Gestione dei Sistemi Informativi adottato dal Confidi è indicata l’attività da svolgere nel caso di problemi relativi alla connettività con il CED del fornitore.

Gestione del documento

Il “Piano di continuità operativa” è gestito dall’ufficio organizzazione e IT che ne cura l’aggiornamento. La revisione è eseguita almeno annualmente a cura dell’Ufficio. Nel caso di cambiamenti importanti nei servizi, nell’organizzazione o per altri casi ritenuti urgenti, la revisione del documento potrà essere effettuata prima della scadenza annuale.

Campo di applicazione

Il documento ha validità per la sede di Scicli (RG), Via dei Lillà 22, nella qualità di centro legale e amministrativo.

Riferimenti normativi

Circolare Banca d’Italia, "Disposizioni di vigilanza per gli intermediari finanziari”, n. 288 del 3 aprile 2015.

Situazioni di emergenza

Sono quelle al verificarsi delle quali Confeserfidi non riuscirebbe ad erogare i servizi ai propri clienti “normalmente”, dovute a qualsiasi evento anomalo, di tipo umano, ambientale, accidentale, doloso, sanitario, socio-politico, ecc.

Glossario

* BCP: Business Continuity Plan: piano di continuità operativa.
* Disastro: evento che causa una grave distruzione in grado di apportare interruzioni alle normali attività aziendali, causando gravi perdite economiche. L’evento può colpire diversi settori come edifici, risorse umane, sistemi informatici, documentazione cartacea, e può causare una quantità di danni ingente, compromettendo a volte pesantemente l’ordinaria operatività dell’impresa e causare gravi perdite economiche.
* Piano di disaster recovery: il piano di disaster recovery è il processo di ripristino dei sistemi informativi inserito nel “Manuale di gestione dei sistemi informativi”. Esso è l'insieme di misure tecnologiche e organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze.
* RTO (Recovery Time Objective) è il tempo necessario per l’attivazione dei sistemi, in caso di disastro, a partire dal momento della sua dichiarazione.
* RPO (Recovery Point Objective) è la distanza temporale tra il momento del disastro e l’ultimo aggiornamento dei dati disponibile sul sito di DR.

# Business Impact assessment

Il sistema “Telematico” è un sistema integrato di Software e database. L’evento catastrofico o il blocco della funzionalità causano il blocco di tutte le attività che vengono eseguite attraverso il sistema stesso.

I processi tecnologici aziendali “on premises” che impattano soprattutto sull’attività commerciale e relativa agli asset di cui al presente documento sono indicati di seguito:

* CRM
* Invio richieste di finanziamento e richiesta di consulenze al confidi
* Protocollo Generale
* Reportistica
* Elenco e gestione pratiche
* Attività di raccolta informazioni AML e verifica delle medesime da parte del’ufficio istruttoria

# Gestione dell’emergenza in fase di crisi o disastro

In Confeserfidi le figure organizzative che intervengono nella gestione degli scenari di crisi sono:

* Consiglio di Amministrazione che, su proposta dell’Amministratore delegato, delibera sullo stato di emergenza. In caso di estrema urgenza la decisione può essere assunta dal Presidente del CdA attivando la procedura di delibera d’urgenza. Il Presidente del Cda informerà il Consiglio alla prima seduta utile.

Su proposta dell’Amministratore Delegato, il Consiglio di Amministrazione può dichiarare la fine dello stato di crisi.

* Amministratore Delegato gestisce lo stato di crisi / disastro e coordina il Comitato.
* Referente continuità operativa: è il responsabile dell’Ufficio Organizzazione e Information Technology che cura la corretta manutenzione e le verifiche del sistema di gestione della business continuity. In condizioni di crisi/disastro, il referente della continuità operativa ha il compito di interfacciarsi con l'Amministratore Delegato e intervenire nel Comitato per la continuità operativa, se convocato dall’Amministratore stesso. Eventualmente il Referente della continuità operativa può suggerire all'Amministratore Delegato se dichiarare lo stato di emergenza e concertare con lo stesso le misure da adottare per fronteggiare lo stato di crisi, compreso l’avvio del processo di disaster recovery dei sistemi.
* Comitato per la continuità operativa: comitato composto dall’Amministratore delegato e dal management aziendale avente il compito di verificare ed approvare tutte le scelte in materia di Business Continuity, ivi compresi gli investimenti necessari.
* Responsabili di Uffici che intervengono nelle valutazioni degli eventi di disastro sull’operatività dei singoli servizi/uffici.

# Valutazione evento ed escalation

Nel presente paragrafo è sviluppato il business continuity plan riferito a tre scenari di crisi principali, così definiti:

1. indisponibilità dell’edificio (**no building**) dove si svolgono processi, dovuta a:

* distruzione dell’edificio a seguito di evento di grossa portata come un terremoto, un incendio, ecc.;
* inagibilità parziale dell’edificio a seguito di eventi di varia natura, con effetti in particolare sull’hardware su cui sono in esecuzione i servizi on premises;
* inaccessibilità dell’edificio a causa di un evento che non rende possibile l’accesso, anche senza compromettere l’integrità dei locali (ad es. blocco della viabilità nell’area dello stabilimento, provvedimenti straordinari in caso di emergenza sanitaria, ecc.).

2. indisponibilità di tecnologia (**no technology**), si considera il caso in cui un ambiente di produzione risulta inutilizzabile in maniera totale o parziale oppure il caso di indisponibilità causata da eventi che compromettono le componenti software ed applicative.

3. indisponibilità di personale (**no people**), si considera l’indisponibilità del personale dedicato ai processi, che può discendere da eventi estremamente diversificati, quali ad esempio: dimissioni in blocco inaspettate, blocco dei sistemi di trasporto, blocco dell’area da parte delle autorità, sciopero generale, epidemie od emergenze sanitarie in genere.

Gestione incidente

In ConfeserFidi, nel caso di evento anomalo, la valutazione dell’incidente avviene secondo la suddetta classificazione.

Il referente della continuità operativa contatta l’Amministratore delegato per valutare la situazione. Insieme stabiliscono se ci sono i presupposti per dichiarare lo stato di crisi.

L’Amministratore delegato propone al Consiglio di Amministrazione la deliberazione dello stato di crisi. In caso di estrema urgenza la decisione può essere assunta dal Presidente del CdA attivando la procedura di delibera d’urgenza.

Su proposta dell’AD, il CDA può dichiarare la fine dello stato di crisi.

## 4.1 Operazioni in caso di scenario no building

In caso di scenario no building, sulla base della tipologia dell’evento, vengono considerati i casi indicati di seguito, inoltre nel caso di indisponibilità prolungata, prevista, del locale, la sede di ripristino, deve essere un locale in uso al Confidi, con connessione alla rete, e viene identificato in ragione della distanza dalla sede centrale, a partire dalla località più vicina geograficamente.

1.1. Indisponibilità temporanea, ad esempio qualche giorno per allagamento, al termine del quale sia possibile rientrare nell’edificio

1.1.1: Se i server (on premises) sono in funzione si può attivare la procedura di smart working

- RTO: nessuno; RPO: nessuno;

1.1.2. Se i server non sono in funzione (non danneggiati, per esempio in caso di assenza di energia elettrica o altro evento che non danneggia i server)

-RTO: tempo di ripristino dei servizi esterni; RPO: nessuno;

1.1.3: se i server non sono in funzione (danneggiati) si avvia la procedura disaster recovery e si torna al punto 1.1.1

RTO: max 48h (nel caso peggiore, cioè acquisto macchina e ripristino totale del contenuto)

RPO: max 24h per il database, max 1 settimana per gli allegati (in questo caso se il server di ridondanza interno è danneggiato, altrimenti 12h)

1.2. Evento disastroso, che comporta l’indisponibilità dell’edificio per un periodo considerevole;

1.2.1. Se i server (on premises) sono in funzione si può attivare la procedura di smart working - RTO: nessuno RPO: nessuno;

1.2.2. Se i server non sono in funzione (on premises), si avvia la procedura disaster recovery presso altro locale, e si torna al punto 1;

1.3. Provvedimenti straordinari in caso di emergenza sanitaria che vietino la mobilità di tutto il personale o parte di esso e comportino l’obbligo di telelavoro per periodi più o meno prolungati nei casi di eventi disastrosi:

1.3.1. Se i server (on premises) sono in funzione si può attivare la procedura di smart working

 - RTO: nessuno; RPO: nessuno;

1.3.2. Se i server non sono in funzione (on premises), si avvia la procedura disaster recovery presso altro locale e si torna al punto 1;

NB: In generale per tutto quel che riguarda l’attività non on premises, cioè servita esternamente in rete on in cloud, l’attività è già per sua natura delocalizzabile quindi fruibile in semplicità in smart working.

##

## 4.2 Operazioni in caso di scenario no technology

Gli scenari di no technology considerati sono i seguenti:

1.1. Indisponibilità completa dei servizi del data center, combinata con no building;

 Vedere il punto 1 no building

1.2. Indisponibilità completa dei servizi del data center, con edificio ancora agibile qualunque sia la causa:

a. evento doloso o vandalico su tecnologia;

b. evento accidentale su tecnologia;

c indisponibilità parziale, ad esempio dei seguenti ambienti:

c.1. Infrastruttura di rete e telecomunicazioni;

c.2. Infrastruttura sw di base, storage;

c.3 architettura applicativa, applicazioni, dbms.

Applicare la procedura di disaster recovery (in particolare nella parte di ripristino software).

RTO: max 48h (nel caso peggiore, cioè acquisto macchina e ripristino totale del contenuto)

RPO: max 24h per il database, max 1 settimana per gli allegati (in questo caso se il server di ridondanza interno è danneggiato, altrimenti 12h)

## 4.3 Operazioni in caso di scenario no people

Gli scenari ipotizzabili sono:

1.1 indisponibilità parziale di personale che ha lasciato l’azienda. In tali casi, l’Amministratore Delegato attiva le azioni necessarie alla riallocazione delle attività e responsabilità sulle risorse di altri uffici, attivando sostituzioni di ruoli anche facendo riferimento anche alle tavole di rimpiazzo. Sarà cura del responsabile di ciascun ufficio aggiornarlo dell’andamento delle attività.

Nel caso in cui invece un dipendente non sia sostituibile dagli altri colleghi (per i più svariati motivi, per es. mancanza di competenze interne), l’AD valuta la possibilità di instaurare rapporti con fornitori o professionisti esterni, anche attraverso la consultazione di lista di società contattabili.

1.2 indisponibilità parziale o totale di personale che non può raggiungere la sede centrale (per es. blocco dei sistemi di trasporto, blocco dell’area da parte delle autorità, sciopero generale, epidemie od emergenze sanitarie in genere). In tali casi si attiva la procedura smart working.

#  Attività connesse

Comunicazione a organi di vigilanza, clienti, fornitori

Per ogni scenario di interruzione viene valutata dall’Amministratore Delegato con il supporto del referente della continuità operativa la necessità di effettuare comunicazione specifica a organi di vigilanza, clienti, fornitori qualora tali eventi compromettano la continuità operativa.

La comunicazione di norma viene inviata ai destinatari dall’Ufficio Affari Generali e Personale.

Comunicazione interna

Per ogni scenario di interruzione, l’Ufficio Organizzazione e IT effettua una comunicazione via email ai responsabili degli uffici del Confidi, indicando i tempi di ripristino previsti.

Inoltre, l’Ufficio Organizzazione e IT si premura di comunicare agli uffici il rientro dallo stato di crisi.

Attivazione procedura di ritorno alla normalità

L’Amministratore Delegato, su indicazione del Referente IT o del Comitato, se convocato, o di altri professionisti eventualmente incaricati, valuta le modalità per ritornare alla normalità che viene deliberato dal CdA.

Una volta ritornati alla situazione di normale funzionamento, l’Amministratore delegato può incaricare di eseguire stime di perdite economiche per eventuali richieste di risarcimenti assicurativi o di altra natura.

Attività periodiche

Il piano di continuità operativa diventa efficace se sono pianificate alcune attività da compiersi a valle dell’approvazione e pubblicazione del documento. Qui di seguito viene data una breve descrizione.

1. test del piano di continuità operativa: Il piano di continuità operativa viene verificato con cadenza minima annuale, per collaudare l’efficienza e l’efficacia delle procedure sviluppate, nelle varie situazioni di crisi che si possono presentare.

2. riesame del piano di continuità operativa: Almeno una volta all’anno o quando sorge la necessità, per cambiamenti aziendali, tecnologici, normativi o legali, è necessario provvedere alla revisione della documentazione, nel principio del miglioramento continuo.

3. verifica di audit: Il documento è a disposizione della Funzione di Internal Audit che dovrà condurre, con frequenza almeno annuale, una specifica attività di controllo in ambito.