PIANO DI CONTINUITA'

Introduzione

La continuità operativa è uno degli strumenti essenziali del business di un'azienda.

Le perdite di un'interruzione dell'attività aziendale sono riassumibili nelle seguenti:

- ✓ Ridotta produttività, nel periodo di interruzione dell'attività e nel successivo lasso di tempo necessario al ripristino;
- ✓ Costi conseguenti alle operazioni di ripresa;
- ✓ Mancato guadagno;
- ✓ Eventuali costi aggiuntivi per spese legali, risarcimenti, ecc.;
- ✓ Danni reputazionali.

Un'impresa, in un'ottica di prevenzione di eventi interruttivi dell'operatività aziendale, mette in campo le risorse che ritiene utili a ridurre la probabilità di accadimento di simili evenienze.

Allo stesso tempo provvede a codificare procedure ed organizzazione necessarie ad affrontare situazioni di emergenza, in modo tale da ridurre al minimo le conseguenze degli stessi, e quindi consentendo il ripristinotempestivo dell'operatività.

La continuità operativa rientra dunque a pieno titolo nella pianificazione aziendale, nell'insieme delle attività che perseguono l'obiettivo di rendere un'impresa pienamente efficiente e competitiva sul mercato.

Premesse

La Società CMS Srl ha sede legale ed operativa a Roma, in via Gela 59.

Essa si occupa di **recupero crediti** per conto di imprese bancarie, finanziarie e commerciali (cd. Mandanti o committenti).

Sul piano pratico, esemplificando, l'operatività aziendale si traduce nelle attività che qui di seguito vengono riassunte.

Le mandanti inviano o comunque mettono a disposizione della Società il carico di lavoro, consistente in pratiche contenenti posizioni debitorie da recuperare presso i debitori; i flussi scaricati sono inseriti nel gestionale interno della Società, installato su server di proprietà della stessa e collocato in sede.

Al server si collegano i diversi pc client su cui operano esclusivamente dipendenti e collaboratori interni.

I dipendenti con mansioni superiori smistano le pratiche da recuperare agli operatori, selezionandole sulla base di alcune variabili (recupero telefonico o domiciliare, area geografica di appartenenza, disponibilità ecc.). Il recupero telefonico (cd. Phone Collection) è effettuato da personale interno; il recupero domiciliare (cd. Home Collection) da agenti della rete esattoriale esterna.

Ciascuno degli operatori affidatari interviene dunque sul proprio pacchetto di posizioni, lavorando come richiesto (tramite attività di contatto telefonico, invio di email o lettere di sollecito, attività di visite domiciliari, ecc.); anche i termini di scadenza delle lavorazioni sono variabili in base a quanto stabilito dalla mandante e/o dalla stessa Società.

L'attività viene svolta con differenti strumenti:

- mediante l'utilizzo di apparecchiature informatiche, di software, di collegamenti telematici e telefonici;
- mediante l'utilizzo di documentazione cartacea, soprattutto per gli esattori esterni, ossia i soggetti che si occupano di Home Collection (e che sono giuridicamente distinti dalla Società, in quanto a loro volta operano per conto di questa, con mezzi ed organizzazione propri).

In entrambi i casi, durante la lavorazione delle pratiche, sul gestionale in uso sono aggiornate le singole posizioni debitorie, mediante l'inserimento di note, di contatti, di evidenze di pagamento, ecc.

I dipendenti con mansioni superiori provvedono, sia nel corso del mandato che alla sua scadenza, ad elaborare report delle attività svolte nel periodo.

Al termine si restituiscono alla mandante tutte le pratiche con la relativa documentazione e gli eventuali effetti di pagamento raccolti.

Finalità del PCO

Il presente Piano di Continuità Operativa (PCO) stabilisce le procedure, l'organizzazione, gli strumenti che consentono alla Società di riprendere la propria attività, in caso di interruzioni dovute ad eventi particolari.
Con il PCO si devono garantire, anche per far fronte a quanto richiesto contrattualmente dalle mandanti, le seguenti condizioni:

a) Elevati costanti livelli di servizio;
b) Minore probabilità di interruzioni dell'attività;
c) Minimi effetti delle interruzioni delle attività;
d) Garanzia del ripristino dei servizi con la maggiore velocità possibile.

Formalizzando le giuste procedure da attivare ed orientando le decisioni corrette da adottare, si ritiene che la Società possa assicurare la continuità operativa, pur in presenza di eventi critici e di situazioni di emergenza.

Prevenzione

Negli ultimi anni, la Società ha elaborato, in questo ambito, un più efficace piano di prevenzione, agendo in particolare sul sistema informatico e sui suoi utenti, con le modalità e gli strumenti che sono di seguito evidenziati:

A. **Ridondanza** (dischi supplementari e schede di rete aggiuntive sul server principale; server secondario delocalizzato; backup multipli; canali di comunicazione e telematici di emergenza);
B. **Sicurezza fisica** (antincendio e climatizzazione dedicate al server principale; chiusura stanza server, accessibile solo a soggetti autorizzati; messa a terra impianto elettrico; Ups dimensionati per le apparecchiature elettroniche);
C. **Sicurezza logica** (accessi limitati e controllati al sistema ed ai dati; sistemi antivirus di tipo professionale, automaticamente e regolarmente monitorati ed aggiornati; filtri antispam; firewall di tipo software);
D. **Formazione del personale** (istruzioni ed affiancamento costanti dell'Ads sulle problematiche sia software che hardware; sessioni formative che coinvolgono anche l'aspetto della continuità operativa).

Modello organizzativo

Il modello organizzativo definisce nel dettaglio ruoli e responsabilità nella continuità operativa aziendale.

Livelli

Nel PCO **il coinvolgimento dei soggetti responsabili della continuità operativa avviene gradualmente**,sulla base dei seguenti due livelli:

1. Livello strategico

Comprende i soggetti che devono **assumere le decisioni**, ossia: Responsabile del PCO e Comitato dicrisi.

Nel dettaglio:

Responsabile del PCO

- contatta il Comitato e, se necessario, gli altri soggetti coinvolti, in caso di crisi;
- contatta il Comitato per le riunioni periodiche di revisione ed aggiornamento del PCO;
- contatta il Comitato per eventuali riunioni straordinarie;
- redige, durante le riunioni, i verbali;
- redige, durante le situazioni di crisi, una relazione sulle attività svolte.

Comitato di Crisi

- decide, supervisiona ed è responsabile della procedura;
- redige, approva e revisiona il PCO;
- valuta le situazioni di emergenza e dichiara, se del caso, lo stato di crisi;
- avvia e controlla le procedure;
- dichiara la chiusura dello stato di crisi;
- coordina le attività formative ed i test annuali.

2. Livello operativo

   Comprende i soggetti che devono **eseguire le decisioni** assunte dal livello strategico, gestendo leattività di continuità operativa e di ripristino.

   Appartengono a questo livello tutti i dipendenti della Società.

Esterni

Tra i soggetti esterni che sono in qualche modo coinvolti dal PCO, vi sono l'Ads ed alcuni fornitori della società.

Business Impact Analysis (BIA)

La Business Impact Analysis (BIA) identifica:

1) i processi critici, ossia quelle attività aziendali che, a causa della rilevanza, richiedono un ripristinoprioritario;
2) gli asset critici, ossia le risorse che sono indispensabili per eseguire i processi critici;
3) le risorse umane critiche, ossia il personale che esegue i processi critici.

Per ciascuno dei processi critici viene indicato il rispettivo tempo di Recovery Time Objective (RTO) e di Recovery Point Objective (RPO), come sarà meglio spiegato in seguito.

Processi critici – Asset – Risorse umane

Sono individuati i seguenti **processi ad alta criticità**:

I. Home Collection (recupero domiciliare)
II. Phone Collection (recupero telefonico)
III. Rendicontazione alle mandanti
IV. Adempimenti di legge

Tali processi utilizzano prevalentemente i seguenti **asset**, tutti presenti presso la sede della Società:

- Server
- Client

- Apparati di fonia
- Connessioni di rete ed Internet

I processi critici individuati impiegano le seguenti **risorse umane** presenti in sede e fuori sede:

- Personale interno
- Esattori esterni

RTO ed RPO

L'RTO rappresenta il tempo che intercorre tra il momento in cui viene dichiarato lo stato di crisi e quello in cui il processo è ripristinato ad un livello di servizio predefinito. E' quindi il **periodo massimo necessario peril ripristino dei servizi/processi critici** della Società.

Per tutti i servizi critici identificati nel precedente paragrafo viene individuato un RTO **massimo di 24 ore**.

L'RPO si ottiene dalla differenza tra il momento in cui il dato viene prodotto e quello in cui viene messo in sicurezza, mediante le procedure di backup adottate dalla Società; rappresenta quindi la **massima perditadi dati tollerata**.

Per tutti i servizi critici identificati nel precedente paragrafo viene individuato un RPO **massimo di 24 ore**.

Scenari di crisi

Gli scenari di crisi sono gli **eventi che richiedono l'applicazione del PCO**.

Vi rientrano sia gli scenari che coinvolgono fisicamente gli asset e/o il personale della Società, sia le situazioni che riguardano i processi, sia infine le emergenze che mettono a rischio l'operatività aziendale complessivamente considerata.

Sono situazioni di emergenza rilevanti ai fini del presente PCO:

1. Indisponibilità o inaccessibilità delle strutture
2. Indisponibilità del personale essenziale
3. Indisponibilità dei sistemi e/o dei dati
4. Interruzione del funzionamento delle infrastrutture

Ognuna delle predette situazioni necessita di una differente reazione, sia in ragione delle conseguenze, sia delle circostanze specifiche (durata; portata; estensione; risorse/asset compromessi e residuali). Conseguenze e circostanze determinano anche la gravità della crisi, la quale si misura con i **livelli** di seguito indicati:

I. Livello 1
   L'evento determina un impatto gestibile con le risorse residue;

II. Livello 2
L'evento determina un impatto significativo ma localizzato;

III. Livello 3
L'evento determina un impatto generalizzato a tutta l'operatività aziendale.

Procedura

La procedura, di responsabilità dei soggetti preposti, deve essere **attivata quanto prima possibile** anche in funzione preventiva di aggravio della portata e delle conseguenze dell'evento interruttivo.

I livelli di gravità di cui al precedente paragrafo devono essere considerati come punto di riferimento, allo scopo di dare le giuste priorità e risposte alle diverse situazioni.

Attivazione

Il soggetto (membro del personale, Ads, amministratore della Società), che riceve una segnalazione o comunque viene a conoscenza di un disservizio che compromette il regolare svolgimento dell'attività operativa ed in particolare dei processi critici aziendali, ne dà **immediata comunicazione al Rco**.

Il Rco esamina la situazione e valuta l'opportunità di attivazione del piano, dichiarando lo stato di crisi, sene ravvisa i presupposti.

Gestione

Dopo l'avvio della procedura, sono **attivati il Comitato di crisi ed il livello operativo**; se necessario sono coinvolti i soggetti esterni competenti (Ads; fornitori).

Di conseguenza sono adottate le decisioni necessarie alla continuità operativa ed al ripristino dello stato preesistente.

Comunicazioni

Nel corso dell'emergenza **i collegamenti con i membri del personale e con l'esterno** (clienti, fornitori, debitori, consulenti, ecc.) **devono essere mantenuti in piena efficienza**.

Potranno utilizzarsi telefoni fissi o mobili, posta elettronica, messaggi, avvisi sul sito della Società.

E' compito del Rco stabilire quali mezzi siano più idonei nelle circostanze del caso, sia per comunicare lo stato di crisi, sia per aggiornare sull'evolversi della situazione, sia infine per avvisare della fine dell'emergenza.

Il contenuto delle comunicazioni deve essere essenziale, diretto e chiaro, espresso con linguaggio semplice ed immediato.

Chiusura

Al termine dello stato emergenziale, devono svolgersi quelle **attività che permettano di tornare ad un livello di operatività almeno pari a quello che precedeva la crisi**.

Solo dopo che sia stata assicurata tale condizione, il Comitato può dichiarare la chiusura dello stato di crisi.

A questo seguiranno la valutazione dei danni generati dall'emergenza e le decisioni in ordine ad un'eventuale revisione del PCO (qualora non si sia dimostrato idoneo ad affrontare l'evento occorso).

Documentazione

Le procedure condotte a partire dalla dichiarazione dello stato di crisi e fino alla sua chiusura devono essere documentate, includendo nelle registrazioni ogni decisione adottata, con le relative ragioni, ed ogni azione eseguita.

Tale documentazione, di responsabilità del Rco, sarà di supporto in sede di revisione annuale del PCO.

Soluzioni di continuità operativa

Agli eventi di crisi individuati nel presente documento (*si veda paragrafo 6)*, devono corrispondere le adeguate soluzioni di continuità operativa che qui di seguito si illustrano, in linea generale.

Indisponibilità o inaccessibilità delle strutture

Si ha indisponibilità o inaccessibilità delle strutture quando queste sono distrutte o non accessibili, come conseguenza di un evento calamitoso.
Ciò può avvenire con riguardo alla sede della Società, laddove sono collocati quasi tutti gli asset e gli strumenti necessari per lo svolgimento dei processi aziendali critici.

Il livello di criticità è il 3.

Preliminarmente si ricordi che la Società dispone di un piano di sicurezza, cui si rimanda per un dettaglio, in forza del quale è necessario seguire le procedure di evacuazione ivi contemplate, al fine di preservare in primis l'incolumità fisica del personale e, secondariamente, gli asset: ciò riguarda in modo specifico gli eventi emergenziali più gravi, quali terremoti, incendi ed allagamenti. La sede rispetta la normativa di sicurezza vigente, disponendo di impianto di messa a terra ed estintori; le apparecchiature elettroniche in uso sono collocate inoltre in posizione rialzata, in modo da evitare il rischio di contatto con liquidi.

La Società, per l'eventualità contemplata nel presente paragrafo, non ha individuato una specifica **sede secondaria di emergenza**; ha tuttavia selezionato alcuni locali, che sono disponibili all'occorrenza, senza necessità di prenotazione e già predisposti con le infrastrutture utili

(collegamenti elettrici, telefonici e telematici). Tali uffici temporanei, situati in diverse zone di Roma, potranno essere scelti in base all'estensione dell'evento, qualora questo coinvolga non la sola sede ma anche l'area in cui essa è situata. In ogni caso ci si è assicurati che ciascuna di queste sedi di emergenza garantisca il rispetto degli obblighi cui la Società è sottoposta (principalmente in materia di sicurezza sul lavoro e di rispetto della privacy).

Nell'eventualità di un simile evento dunque il Rco, dichiarato lo stato di crisi e convocato il Comitato, provvede alle operazioni conseguenti.

Per il tramite del livello operativo, dovrà coinvolgersi l'Ads, per la connessione al **server secondario** che corrisponde, ad ogni livello (software di base, applicativi ed impostazioni di sicurezza), al server primario presente in sede.

Quanto alla **componente dati**, il server secondario è sincronizzato con il principale, per cui dispone anche del database utile alla prosecuzione del lavoro di recupero crediti.

Sarà dunque l'Ads a curare il passaggio dal server principale a quello secondario, con le seguenti operazioni:

- comunicazione del nuovo indirizzo IP al personale della Società, per la connessione in desktop remoto;
- verifica del corretto allineamento dei dati (che, come si è detto, sono già presenti sul server secondario);

Alcuni membri del personale hanno in dotazione **personal computer** utilizzabili nella sede di emergenza, presso la quale dovranno essere trasferiti. Tali dispositivi sono già dotati di ogni configurazione utile alla ripresa dell'attività operativa e delle impostazioni di sicurezza necessarie alla protezione del sistema e dei dati. Se dovesse rendersi necessario, la Società provvederà all'acquisto o al noleggio di ulteriori dispositivi, per i quali interverrà l'Ads al fine di effettuare le operazioni di messa in sicurezza e di connessione al server.

Allo stesso tempo sono a disposizione del personale alcuni **telefoni mobili** con i quali è possibile mantenere le comunicazioni con fornitori, clienti ed esattori esterni: a costoro dovrà darsi avviso della situazione di emergenza occorsa, indicando indirizzo della sede alternativa prescelta e numeri di contatto utili. Tale avviso potrà essere dato telefonicamente, a voce, oppure via mail, o ancora tramite messaggistica istantanea (SMS o Whatsapp), non appena ci si è insediati nella sede di emergenza.

Interruzione dei servizi essenziali

Quando vi è un'interruzione del funzionamento delle infrastrutture (elettricità, rete interna, telefonia e/o internet) si delineano diversi scenari, con livelli di criticità differenti, a seconda della durata e gravità dell'evento e degli impatti conseguenti.

Il Rco, informato dell'evento, provvede alla gestione dell'emergenza, operando in prima persona o, previa dichiarazione dello stato di crisi, attivando il Comitato ed il personale di supporto.

Interruzione elettricità

Le attività essenziali dell'azienda richiedono l'utilizzo di strumenti alimentati da corrente elettrica, per cui la sua mancanza (non meramente temporanea) può arrivare a determinare uno scenario con livello di gravità 3.

Il Rco, dopo aver verificato l'entità e la causa dell'evento, agisce di conseguenza: potrebbe dover chiedere l'**intervento di un tecnico**, qualora l'interruzione sia motivata da problematiche interne; in caso contrario, dovrà rivolgersi al fornitore, anche per conoscere i tempi di risoluzione del guasto.

In caso di notevole prolungamento dei tempi di riattivazione della linea elettrica, si potrebbe dover ricorrere alla dichiarazione dello stati di crisi e persino alle medesime azioni previste per l'indisponibilità o inaccessibilità delle strutture (*si veda quanto indicato nel precedente paragrafo*).

N.B.: il livello operativo, in tale situazione emergenziale, è tenuto a procedere al corretto spegnimento del server; questo è infatti collegato ad un Ups che assolve alla funzione di mantenere il dispositivo acceso per un lasso di tempo sufficiente ad eseguire le regolari operazioni di arresto del sistema.

Tale precauzione mira a scongiurare che vi siano danneggiamenti alle componenti del server ed ai dati, possibili in caso di spegnimenti improvvisi.

Interruzione linea telefonica

Venendo a mancare la linea telefonica fissa della sede, in ogni caso (guasto interno o imputabile all'operatore o alle infrastrutture locali di riferimento), lo scenario rappresenta solo un disagio, non determinando un totale blocco delle comunicazioni.

Il livello di criticità è dunque 1.

Alcuni membri del personale sono dotati di **telefoni mobili** comunemente utilizzati anche in normali condizioni di operatività; gli esattori esterni dispongono di propri mezzi di comunicazione.

La mancanza della linea fax potrà essere facilmente supplita dall'invio/ricezione di mail.

Accertato il guasto, il Rco dovrà contattare l'**operatore di riferimento** (anche per isolare la causa); di seguito, se il guasto è interno, dovrà contattare un tecnico.

Nel frattempo è fondamentale che si dia avviso della problematica e delle modalità di comunicazione alternativa al personale ed agli altri contatti rilevanti.

Tale avviso potrà essere dato telefonicamente, a voce, oppure via mail, o ancora tramite messaggistica istantanea (SMS o Whatsapp).

Analogo avviso verrà rilasciato nel momento in cui la linea torni ad essere operativa.

Interruzione linea internet

La mancanza di linea internet impedisce le comunicazioni telematiche della Società con l'esterno.

Resta tuttavia attiva la connessione intranet, ossia della rete interna e quindi anche l'operatività sul server, sul gestionale e sui dati.

Per quei processi critici che richiedono le comunicazioni telematiche, la Società dispone di una **connessionedi emergenza** tramite rete 4G.

La situazione non coinvolge gli esattori esterni.Il livello di criticità si attesta su 1.

Accertata la suddetta criticità, il Rco, segnala il guasto all'operatore di riferimento; se dovesse riscontrarsiche la causa del disservizio è interna, di competenza della Società, interviene l'Ads.

In ogni caso il livello operativo, eventualmente con il supporto dell'Ads, verifica il funzionamento della rete4G, già configurata.

Indisponibilità del personale

In questo PCO non viene presa in considerazione un'assenza massiva di tutto il personale, che è da considerarsi evento non realistico; la **mancanza di uno o più membri** può essere compensata dal lavoro di altri operatori, ciascuno per quanto di propria competenza.

Per le operazioni di maggiore responsabilità, qualora manchino i soggetti incaricati, interviene l'amministratore.

Per quanto concerne gli esattori esterni, l'eventuale mancanza di uno o più di essi, determina una situazione più problematica, ma ugualmente risolvibile.

Si ravvisa un livello 2 di criticità.

Il Rco contatta gli esattori esterni disponibili che possono sostituire più agevolmente gli assenti, in considerazione delle distanze geografiche e degli impegni già assunti; qualora non vi sia disponibilità, il Rco contatta altri abituali collaboratori e formalizza l'incarico a quelli che si mettono a disposizione.

Interruzione dei sistemi informativi

Nel presente PCO si esaminano esclusivamente gli **eventi che causano totale indisponibilità degli apparati informatici o del gestionale** in uso; non sono ricompresi gli eventi che causano meri inconvenienti che, seppur significativi, non bloccano l'operatività aziendale.

L'interruzione dei servizi informativi richiede l'intervento dell'Ads, che verifica il guasto ed effettua il necessario intervento tecnico.

Durante il blocco, il Rco comunica al personale la circostanza: ciascun membro è tenuto ad annotare su carta le operazioni compiute, che all'avvenuto ripristino dovranno essere riportate sul sistema.

Revisione	Data	Contenuto
Rev. 0	Luglio 2019	Prima redazione
Rev. 0.1	Luglio 2020	Conferma
Rev. 1	Settembre 2020	Modifiche introdotte a seguito di implementazione di backup in cloud
Rev. 1.1	Settembre 2021	Conferma
Rev. 1.2	Settembre 2022	Sostanziale conferma
Rev. 2	Settembre 2023	Revisione del documento per: - introduzione di nuovi apparati e servizi informatici (server; cloud); - nuovo RCO e Comitato di crisi