PIANO DI DISASTER RECOVERY (DRP)

Il piano di disaster recovery (DRP) è parte integrante del PCO.

Il suo scopo è di **illustrare le misure tecniche ed organizzative che assicurano il funzionamento ottimale del sistema informativo della Società**.

Premesse

La Società utilizza un sistema informativo che si struttura su alcune fondamentali componenti e caratteristiche di seguito elencate.

Hardware

Gli asset hardware sono prevalentemente collocati presso la sede della Società; alcuni dispositivi supplementari e di emergenza, come accennato nel PCO, sono tuttavia delocalizzati.

In sede è presente il **server**, sul quale sono installati gli applicativi e dove vengono anche allocati tutti i dati.

Il server si trova in una apposita stanza, chiusa a chiave ed accessibile solo al personale autorizzato; l'Ads vi accede solo previa autorizzazione di chi detiene le chiavi e registrazione dell'accesso. Nella stanza viene mantenuta una temperatura il più possibile stabile, allo scopo di evitare che eventuali sbalzi determinino danni ai componenti; è inoltre disponibile un estintore dedicato.

Un gruppo di continuità dimensionato è collegato al server, allo scopo di mantenere costante la corrente in ingresso e di poter spegnere regolarmente il dispositivo in caso di black-out.

Il server è dotato di componentistica ridondante: oltre a due schede di rete, sono presenti due dischi in modalità Raid; quest'ultimo sistema consente, in caso di rottura o malfunzionamento di uno dei dischi, di proseguire l'attività sul server, semplicemente staccando il componente danneggiato.

Nel mese di agosto 2023 è stato completato il processo di sostituzione del server con un nuovo apparato di maggiore efficienza ed affidabilità.

La ridondanza non riguarda solo i componenti del server ma tutta la struttura hardware, in quanto una perfetta replica del server è collocata, come detto, in altra sede.

Questa precauzione consente di proseguire l'attività operativa dell'azienda anche in caso di indisponibilità o inaccessibilità della sede, o nell'eventualità di rottura del server principale.

Infatti l'accesso al gestionale, installato su entrambi i server, necessita solo di una connessione in desktop remoto, che sarà di pressoché immediata realizzazione, richiedendo solo un collegamento ad un differente indirizzo IP da parte dei client.

Software

Il **gestionale** per l'attività di recupero crediti, denominato Uno, è il principale strumento di lavoro software della Società: qualora esso fosse indisponibile, si avrebbe un blocco totale dell'operatività aziendale.

Tale programma è stato realizzato su misura dallo stesso Ads, che provvede anche agli aggiornamenti, alla risoluzione delle problematiche e ad ogni altra attività di supporto: i suoi interventi vengono eseguiti sia in presenza che da remoto, come del resto avviene anche per ogni altra sua assistenza sul sistema informativodella Società.

Le operazioni di manutenzione sono in genere programmate ed eseguite in orari e giorni di chiusura; eventuali interventi in emergenza sono effettuati prontamente, se non rinviabili.

Vi è tuttavia da precisare che il software di cui trattasi non ha in passato manifestato particolari problematiche di funzionamento, risultando nel complesso stabile ed efficiente.

Linee telefoniche e telematiche

I dispositivi che consentono i collegamenti telefonici e telematici (centralino, telefoni fissi e mobili, router, collegamenti, switch ed accessori vari) sono collocati ugualmente presso la sede della Società.

L'infrastruttura telefonica e telematica è ridondante per la presenza, già accennata, di un operatore per la telefonia fissa e la fibra, cui si aggiungono la connessione 4G ed alcuni cellulari aziendali, che consentono di supplire ad eventuali interruzioni della linea principale, sia per la parte telefonica che per la connessione dati.

Infrastrutture

Essendo la sede della Società unica ed essendo in essa collocati tutti gli asset principali per l'operatività aziendale, eventuali criticità infrastrutturali che dovessero interessare gli uffici sono da misurare con **differenti livelli di gravità**, in ragione dell'evento emergenziale e dei conseguenti impatti.

Backup e ripristino dei dati

La continuità operativa della Società si garantisce anche attraverso una corretta procedura di salvataggio e successivo ripristino dei dati essenziali alla stessa operatività.

Tale essenzialità investe in primo luogo i dati che derivano dalla lavorazione delle pratiche di recupero credito e quindi dal gestionale in uso; in secondo luogo include la posta elettronica, la

contrattualistica, i documenti inerenti i rapporti con il personale e con gli esattori esterni e quelli relativi alle attività amministrative e di segreteria.

Si tenga presente che, negli ultimi anni, per ragioni di spazio e di risparmio in termini economici ed ecologici, la Società ha progressivamente diminuito il volume del cartaceo ed ha correlativamente provveduto a scansionare la gran parte dei documenti esistenti. Ciò ha contribuito ad una maggiore efficienza, in quanto allo stato i dati sono per la gran parte digitalizzati ed in quanto tali, sono più facilmente archiviabili e reperibili.

Tutti i dati digitali risiedono sul server, su entrambi i dischi, che sono in modalità Raid e quindi entrambi utilizzabili anche separatamente: in caso di guasto di uno dei due, l'immagine dell'altro assicura la perfetta integrità anche dell'archivio.

Il **salvataggio principale** dunque avviene in modalità sincrona, ossia in tempo reale su ciascuno dei due dischi.

Sono poi previste **ulteriori operazioni di backup differenziate** sia per la destinazione, che per le modalità, sia infine per l'oggetto. Tutte sono eseguite in diversi orari, in ogni caso dopo la chiusura degli uffici, allo scopo di evitare un sovraccarico di lavoro del sistema che ne determinerebbe il rallentamento e l'efficienza.

1. I dati amministrativi, di segreteria e le mail sono salvati quotidianamente su un Nas collocato nellastessa sede della Società. Il salvataggio in questo caso è di tipo asincrono ed incrementale.
2. I dati del gestionale sono salvati, quotidianamente, sul server remoto secondario delocalizzato. In questo caso il backup avviene in maniera sincrona ed incrementale.
3. Tutti i dati sono infine salvati quotidianamente in cloud, sempre con modalità asincrone e semprein maniera incrementale.

Quest'ultimo salvataggio si è reso necessario per una maggiore sicurezza e per poter disporre dei dati di amministrazione e segreteria e di quelli riguardanti il personale, anche al di fuori degli uffici, nel caso in cui si verifichi un evento che renda la sede inaccessibile.

Il servizio cloud è stato peraltro sostituito con altro più efficiente ed affidabile nel 2023.

Formazione ed esercitazioni

La gestione di un'emergenza può non essere semplice, per cui il Rco organizza, almeno annualmente:

- Attività formativa teorica;
- Esercitazioni pratiche.

La prima attività formativa è avvenuta nel Settembre 2019, a beneficio di tutto il personale interno della Società.

Nel successivo mese di Dicembre è stata effettuata una prima esercitazione sulla procedura in caso di inaccessibilità/distruzione delle strutture; durante la simulazione si è resa evidente la problematica del salvataggio dei dati di amministrazione e segreteria: per tale ragione si è dunque optato, dopo un periododi riflessione, per un backup in cloud.

Una seconda attività è stata effettuata nel mese di luglio 2021, in ritardo a causa degli eventi legati alla pandemia da Covid-19, che hanno determinato un allungamento dei tempi previsti. Non sono state rilevate particolari necessità per cui nella redazione della versione aggiornata del PCO si è deciso di confermare quanto previsto lo scorso anno.

Ulteriore attività di verifica è stata eseguita nel luglio 2022: anche in tal caso si è confermato sostanzialmente il presente documento.

Nel 2023 è stato introdotto un nuovo server per cui le attività di test sono state condotte nel mese di agosto per verificare che le innovazioni non determinassero esigenze di modifiche nelle procedure di continuità operativa e disaster recovery; i controlli non hanno evidenziato criticità.

Aggiornamento del PCO

Il PCO è revisionato almeno annualmente. Modifiche ed integrazioni sono effettuate anche nel caso in cui vi siano significativi cambiamenti nelle infrastrutture e nelle apparecchiature in uso, oltre che nell'operatività aziendale.

La tabella seguente contiene indicazioni sulla redazione e revisione del PCO nel temp

Revisione	Data	Contenuto
Rev. 0	Luglio 2019	Prima redazione
Rev. 0.1	Luglio 2020	Conferma
Rev. 1	Settembre 2020	Conferma
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

C.M.S. s.r.l. - Via Gela, 59 - 00182 Roma - Tel.: 06/70305612 - 06/70302018 - Fax 06/89280732
e-mail: info@cmsdomus.it - PEC: cmssrl040@lamiapec.it - R.E.A. 724768 - P.IVA 04040641005

Il presente verbale si redige a seguito delle operazioni di teste verifica del Piano di continuità operativa PCO e del Disaster Recovery effettuato dalla Società in data 30/08/2023, a seguito dell'introduzione del nuovo server primario e delle conseguenti attività di configurazione dei servizi, utenze, connessioni e backup.

Le operazioni di test sono avviate alle ore 9:00.

Si simula la mancata accensione del server,con conseguente indisponibilità dei servizi informatici principali, in modo particolare del gestionale di recupero crediti in uso, denominato "Uno", installato sul predetto server e fruibile dalle postazioni client mediante connessione in desktop remoto.

Il personale rileva l'inaccessibilità delle risorse installate sul predetto server e la comunica alle ore 9:10 al Responsabile della Continuità Operativa (RCO).

Dopo aver accertato la problematica principale, il RCO contatta il responsabile dei sistemi informatici della Società.

Si valutano di conseguenza le seguenti due opzioni:

1. Prioritario intervento in sede del responsabile dei sistemi informatici, per gli approfondimenti tecnici necessari e la risoluzione del guasto del server;
2. Prioritaria messa in funzione del server virtuale secondario delocalizzato, sito presso diversa sede,in attesa del successivo ripristino del server principale, quindi con posticipazione dell'intervento tecnico on site.

Vengono calcolate le tempistiche approssimative necessarie all'una ed all'altra opzione, valutate come di almeno 5/6 ore per la prima e di un massimo 1 ora per la seconda.

Di conseguenza il RCO valuta come preferibile la soluzione 2, che consente una più rapida ripresa delle attività, ed incarica quindi il responsabile dei sistemi informatici delle operazioni necessarie nell'immediato all'attivazione e connessione del server secondario, nonché di quelle che in seconda battuta dovranno eseguirsi per la riparazione del server principale.

Alle ore 9:30 il RCO dichiara lo stato di crisi, formalizzandone il livello 2, ed attiva il Comitato di crisi ed il livello operativo.

Il Comitato di crisi provvede alle comunicazioni necessarie verso il personale e gli agenti esattoriali della rete esterna, rispettivamente di persona e mediante telefonata o messaggio telefonico.

Tutti i soggetti risultano essere stati informati entro le ore 9:45.

Le attività operative sono sospese, salvo per quanto sia eseguibile in assenza delle risorse informatiche inaccessibili; restano regolari le comunicazioni telefoniche, la connessione ad Internet e l'accesso alla posta elettronica tramite Webmail.

La ricezione di telefonate o mail da parte di debitori viene gestita regolarmente dagli operatori, per quanto sia possibile in assenza del gestionale.

Di ogni operazione il personale tiene traccia in ogni caso, mediante annotazione manuale.

Il completamento delle attività di attivazione e connessione del server secondario ha richiesto un tempo di 35 minuti; le operazioni hanno richiesto il collegamento dei pc client con il server secondario, mediante sostituzione, sui pc in uso, dell'indirizzo IP del server primario con quello del suo sostituto.

Sono stati impiegati ulteriori 12 minuti per la verifica dell'allineamento delle utenze e dei dati.

Alle10:25 il sistema ha ripreso il normale funzionamento, attestando il RTO a 1 ora e 25 minuti.

Il RPO è stato nullo, in quanto il server secondario è sincronizzato con il principale, sia per la configurazione che per la componente dati.

La chiusura dello stato di crisi è avvenuta alle ore 11:00, dopo che il RCO ha verificato che ogni aspetto dell'operatività aziendale non manifestasse problematiche.

Il comitato di crisi ha avvisato il personale e gli esattori esterni della cessazione dell'emergenza con le medesime modalità con cui aveva provveduto a segnalare l'evento.

Tutti i suddetti soggetti sono stati invitati a riportare sul gestionale eventuali annotazioni manuali effettuate nel corso della procedura.

Non si sono manifestate criticità nel corso del test.

Roma, 30/08/2023