C.M.S. SRL

Piano di Disaster recovery

Nell'unica sede di Via Gela, 59, sono trattate diverse banche dati, elettroniche e cartacee, per la salvaguardia delle quali sono stati implementati diverse tipologie di misure di sicurezza.

In linea di massima, architetturalmente, il sistema informativo è composto da 4 siti:

- **La rete locale dell'ufficio**
- **Lo studio del Commercialista**
- **L'hosting della posta elettronica**
- **Un sito in hosting di parte per i backup esterni.**

Sul file server sono archiviati i dati non strutturati (documenti raggruppati in cartelle catalogate per categoria ed anno) e la banca dati dell'applicativo gestionale in estensione DBase/Visual FoxPro per la gestione del business (pratiche, anagrafiche, piani di rientro, scadenziari attivi e passivi, estrazione timesheets e consuntivazione, fatturazione, reporting). La contabilità effettiva oltre alle varie dichiarazioni ed i libri contabili sono tenuti presso lo studio del commercialista.

Non c'è un server di posta interno, solo mailbox in hosting. I messaggi fluiscono direttamente dalle mailboxes POP3 esterne agli account in Outlook. Su Outlook è stata abilitata l'archiviazione automatica settimanale per cui ogni account dispone di un file PST primario e di uno di archivio; il file primario rimane di piccole dimensioni mentre l'archivio cresce fino a raggiungere il gigabyte per alcuni account.

Il profilo di ogni Client di posta viene memorizzato in una apposita cartella che lo identifica all'interno di una directory del file server.

Gli applicativi gestionali sono disponibili al funzionamento, mediante semplici icone presenti sul desktop del pc client di ogni operatore autorizzato all'utilizzo.

Nello studio di fattibilità tecnica, si è tenuto presente che lo studio del commercialista, come tutti i studi professionali in genere, non dispone di un piano di disaster recovery. Nel nostro caso il problema coinvolge alcuni documenti ricevuti in formato cartaceo (normalmente fatture passive, scontrini, ricevute, etc.) . Ognuno di questi documenti viene digitalizzato (scanner) e salvato nel file-server, prima dell'invio allo studio professionale. In caso di disastro presso lo studio professionale dovranno essere ricostruiti i libri contabili prelevando le informazioni dal repository documentale presente nel file-server; le informazioni raccolte andranno poi ad integrarsi con l'ultima copia dei libri depositati presso la sede sociale.

Il piano di backup prevede la clonazione mensile dell'immagine dei dischi del server su un NAS esterno, mantenendo a rotazione tre immagini mensili, tramite applicativo *Clonezilla*.

Il mantenimento del servizio di posta elettronica è garantito dal servizio di hosting.

Le immagini delle stazioni di lavoro vengono salvate mensilmente mediante Windows Backup su disco esterno.

I backup dei server e delle immagini delle stazioni di lavoro avvengono a caldo; sono completamente automatizzati e controllati mediante il servizio di monitoraggio interno che segnala

via email eventuali problemi riscontrati durante il processo. In ogni stazione di lavoro è presente l'applicazione *Cobian Backup* per il salvataggio schedulato giornaliero (o quando si ricollega il portatile alla rete locale) della raccolta "documenti" e della cartella "Desktop", (la mailbox Outlook è già allocata su server). *Cobian* viene lanciato automaticamente come servizio di sistema all'avvio della postazione e crea su disco NAS esterno, un archivio zip nominato client-aaaa-mm-gg, lasciando a disposizione dell'utente il salvataggio per 30 giorni. La leggibilità dei supporti di backup viene verificata ogni mese mediante ispezione manuale.

Il piano include un'inventario dei sistemi, delle applicazioni e delle informazioni. Questo è un estratto

Sistema	Caratteristiche	Tipo	Locazione	Ripristino Rapido	Resilienza	RTO	Note
Server	Server Dell	Windows 2008 R2	On-site	Acquisto Configurazione	A	A B	Prioritario
NAS	Synology Disk Station *DS710+*	CIFS/SMB	On-site	Acquisto Configurazione	A	A A	Prioritario
Direzione	Pc Client	Windows 7 Pro	On-site	Acquisto Configurazione	A	A A	
Segreteria 1	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
Segreteria 2	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
Segreteria 3	Pc Client	Linux	On-site	Acquisto Configurazione	A	A A	
Segreteria 4	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
Segreteria 5	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
Segreteria 6	Pc Client	Windows 2008	On-site	Acquisto Configurazione	A	A A	
Segreteria 7	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
Segreteria 8	Pc Client	Windows XP	On-site	Acquisto Configurazione	A	A A	
SEDE	Documentazione Tecnica\Layout_planimetria_cr.doc	Ufficio	On-site	Affitto temporaneo Allestimento	A	C B	Prioritario
APPARATI DI RETE	Router Telecom, switch di rete 24 porte Gigabit, prese di rete cablate	Apparati di rete	On-site	Acquisto Configurazione	A A	A A	Inclusi in sede temporanea

LEGENDA	
Resilienza	A= Non resiliente B= Resiliente, ripartenza in minuti C=Resiliente, nessuna interruzione di servizi
RTO	A=entro le 4 ore B=da 4 a 24 ore C=da 1 a 5 giorni D=Più di una settimana

Tutti i Pc-Client sopra elencati lavorano prevalentemente in connessione Desktop Remoto con il server, ognuno con la propria password di accesso (conforme ai requisiti di complessità).

Piano di ripristino

Il sistema informativo non è soggetto a vincoli normativi o contrattuali che impongano livelli di servizio minimi al di là di quelli imposti dal D.lgs. 196/2003 (Disaster Recovery Plan e D.LGS 196/2003); ne consegue che la determinazione dei parametri di RTO e RPO sono stati lasciati al buon senso. L'idea di base è stata quindi di utilizzare il sito in hosting per il disaster recovery della società e di appoggiare il DR del sito in hosting su qualche servizio "in the cloud"; visto che disponiamo di un account, aperto precedentemente su Altervista, abbiamo deciso di utilizzare questo.

Il primo problema affrontato, è stata la scarsa disponibilità di banda in upload.

L'upload dei documenti (3.5 GB tot) ha richiesto circa 17 ore per il primo trasferimento; poiché si è trattato di una operazione non presidiata (unattended), è stata avviata e conclusa nel giro di un fine settimana. Le sincronizzazioni giornaliere trasferiscono poco più di qualche decina di MB.
I database occupano poco più di 8GB ma la compressione ha ridotto l'occupazione a poco più di

350MB.

Anche il primo trasferimento degli archivi Outlook ha richiesto circa 22 ore, realizzato in un weekend. Utilizzando il protocollo RSYNC con funzioni elementari di deduplicazione (invio dei soli blocchi modificati) su un tunnel SSH con una ADSL a 7Mb/sec (upload 480 Kb/sec), abbiamo ottenuto un notevole miglioramento dei tempi di trasferimento, aggiornando il backup esterno di volumi di file da 1Gb a circa 60/70kB/sec: per esempio, l'invio dei soli blocchi modificati di un file PST da 1GB riduce i tempi di aggiornamento dalle 5 ore previste a qualche minuto.

Per l'esecuzione dei salvataggi si procede come segue:

1) Backup dei dati critici delle stazioni di lavoro via sincronizzazione di cartelle con il server (Cobian già in opera).

2) Backup giornaliero dei dati critici del server mediante sincronizzazione con il sistema in hosting di (RSYNC):

a) Cartella dati critici delle stazioni di lavoro.
b) Cartella dei backup pianificati degli archivi del gestionale per il Recupero Crediti.
c) Cartella del repository documentale.
d) Cartella delle configurazioni.

3) A fine aggiornamento le vecchie copie più vecchie di 30 giorni vengono eliminate, lasciando disponibile per un'archiviazione storico, l'ultimo backup del mese.

Sicurezza

Nel nostro lavoro non trattiamo dati sensibili; tuttavia possiamo venire in possesso di alcune informazioni critiche per i nostri clienti che in ogni caso teniamo a proteggere. Per questa ragione la cartella "Documentale" e la "Recupero crediti DBF" non sono incluse direttamente nel normale ciclo di sincronizzazione via RSYNC, ma viene prima inviata ad una normale cartella compressa (.zip) e cifrata via GPG ; tutto questo prima che parta il normale processo di sincronizzazione.

Le chiavi GPG sono protette da un processo ad-hoc.

Costi

Ogni mese ci vengono addebitati circa 1,5€ per 1GB di spazio occupato e circa 16GB/mese di trasferimenti. Il numero di operazioni non è significativo.

Conclusioni

Il piano così implementato è classificabile secondo i seguenti parametri:

RPO: Classe B: max 8 ore lavorative.

RTO: Classe B: da 4 a 24 ore solari.

BS7799-2 MTPD (Maximum Tolerable Period of Disruption): NA.

C.M.S. SRL – VIA GELA 59, 00182 ROMA

TEL. 06/70305612-06/70302018 FAX 06/89280732

info@cmsrecuperocrediti.it www.cmsrecuperocrediti.it

cmssrl040@lamiapec.it

R.E.A. 724768 P.IVA 04040641005