

Rodinò & Partners

Business Continuity Plan

Ed.01/2019

CONSIDERAZIONI PRELIMINARI:

- gli uffici si trovano al 5° ed ultimo piano; il terrazzo/solaio di copertura è stato recentemente completamente ristrutturato con rifazione di tutti i massetti e applicazione di tre strati di guaina
- il fabbricato ha subito negli ultimi 5 anni importanti lavori di consolidamento strutturale ed antisismico
- l'ufficio ha un'unica porta d'ingresso rinforzata e sorvegliata da 3 telecamere (1 interna ,2 esterne) con registrazione delle immagini e possibilità di visione in remoto.
- tutto il cablaggio (sia dell'ufficio che del fabbricato) è di recente installazione e completamente canalizzato
- il 90% dell'archivio "vivo" è in formato digitale e quindi riveste una limitata importanza l'eventuale distruzione dell'archivio cartaceo
- tutti i dipendenti e collaboratori sono in grado, previa comunicazione delle password, di accedere al server aziendale dalle proprie abitazioni in quanto dispongono di un collegamento ad internet via ADSL e possono quindi lavorare anche da casa
- in caso di indisponibilità dell'ufficio è possibile usufruire temporaneamente delle seguenti locations alternative tutte dotate di collegamento ad internet:
 - o Via Bisignano 11 - Napoli (quartiere diverso di quello dell'ufficio)
- La R&P dispone della seguente infrastruttura informatica:
 - o Server Fujitsu TX2540 M1 E5-2407V2 8GB 4LFF con 4 HD da 1 TBII server viene cambiato ogni 2 anni ed è collegato in rete con 11 client, il dominio è gestito dal server.
 - o Negli ultimi 10 anni non si è mai verificato alcun problema relativo alla sicurezza dei dati.
Il server dispone di vari livelli di protezione contro attacchi informatici(firewall HW, VPN Access)
 - o Windows Server 2012
 - o Programma gestionale Pass Broker (gestione polizze e sinistri) e Pass Coge (contabilità) della RGI spa di Ivrea che è il principale fornitore di Brokers italiani
 - o Viene eseguito il back-up incrementale giornaliero ed uno settimanale completo su uno spazio Cloud gestito da GOOGLE.
 - o La connessione internet e telefonica è fornita da Fastweb 100 mega con sistema FTTH (fiber to the home)
 - o Per i servizi principali (server,centralino telefonico,illuminazione di sicurezza etc.) Sono presenti gruppi di continuità per consentire un temporaneo regolare funzionamento anche in caso di black-out.

INDIVIDUAZIONE RISCHI:

- Impossibilità accesso ufficio
- Distruzioni fisiche di beni strumentali
- Indisponibilità risorse umane
- Attacchi informatici
- Blackout elettrico/rete

CAUSE:

- Terremoto, eruzione vulcaniche ed altri avvenimenti catastrofici
- Incendio e scoppi
- Allagamenti
- Furto
- Epidemie
- Atti vandalici e Sociopolitici

COMITATO DI CRISI:

- U. Rodinò
- Gabriella Stanzione
- Francesco Izzo della Brk srl (responsabile Ced con uffici a Padova)
- Guido Izzo, corrispondente a Napoli di Brk srl
- Ing. Lucio Cappelli (esperto in statica e direzione lavori)

PROCEDURE DI CONTINUITÀ:

- Riunione immediata del comitato di crisi
- Valutazione delle cause, dei danni ,dei probabili tempi di ripristino ed in particolare verificare la possibilità di continuare a lavorare dall'ufficio e controllare le funzionalità della rete e del server.
- Mettere sull'avviso il personale eventualmente assente o non a conoscenza dell'avvenimento
- A questo punto si aprono due opzioni a seconda se sia o meno efficace il collegamento alla rete e al server :

A.

B. Regolare funzionamento della rete e del server

- Utilizzando le mailing list disponibili avvisare immediatamente Clienti e Compagnie tramite il server di posta elettronica (con eventuale accesso in remoto)



- Decidere eventuale location alternativa; in caso di danno grave i dipendenti potranno continuare a lavorare da casa collegandosi in remoto al Server previa comunicazione dei codici di accesso.



- Riprendere attività ,sia pure in condizioni disagiate, sino al completo ripristino della normale attività

B. Interruzione del collegamento alla rete e al server

- Avvisare Clienti e Compagnie via email attraverso l'utilizzo dell'account email @rodino.it tramite il provider Google



- richiedere a Francesco Izzo di Brk di attivare immediatamente il Server sostitutivo già preinstallato presso il Suo ufficio di Padova con inserimento dei dati dal back-up remoto (tempo stimato: 2 giorni lavorativi)



- Decidere eventuale location alternativa; in caso di danno grave i dipendenti potranno continuare a lavorare da casa collegandosi in remoto, non appena riattivato, al Server sostitutivo.



- Riprendere attività ,sia pure in condizioni disagiate, sino al completo ripristino della normale attività

Nota: annualmente viene effettuato un test per simulare una situazione di crisi e verificare l'efficacia delle procedure di salvataggio