CONVENZIONE INTERBANCARIA
PER I PROBLEMI DELL'AUTOMAZIONE

GRUPPO DI LAVORO

CONTINUITA' DI SERVIZIO E GESTIONE DELL'EMERGENZA

MAGGIO 2000

In relazione alle indicazioni contenute nel Piano delle attività della CIPA per il periodo 1.1.2000 - 30.6.2001, il gruppo di lavoro “Continuità di servizio e gestione dell’emergenza” rassegna il proprio rapporto.

La Segreteria della Convenzione desidera ringraziare i componenti del gruppo di lavoro di seguito indicati per la collaborazione prestata e il contributo fornito nello svolgimento delle attività del gruppo:

Andrea	CIVIDINI	BANCA D’ITALIA (Coordinatore)
Domenico	BERARDI	BANCA D’ITALIA
Alessandro	ZOLLO	ABI
Franco	MASERA	SANPAOLO - IMI
Antonio	PELUSO	BANCA DI ROMA
Gianpaolo	BORGHI	CREDITO EMILIANO
Roberto	POZZUOLO	BANCA SELLA
Gian Paolo	BATTISTELLA	BANC POP. COMM. E INDUSTRIA
Gabriele	BELLATO	BANCA INTESA
Marcello	COSTA	SIA
Davide	POZZO	SSB
Fabio	ROMANI	SECETI
Antonio	CUSANO	ICCREA
Luciano	VANNI	ICCRI
Francesco	RUOTOLO	ICCRI

Il riconoscimento va esteso ai numerosi colleghi del Servizio Elaborazioni e Sistemi Informativi della Banca d’Italia, in particolare al dr. Fabio Fillo e all’ing. Silvio Orsini, che hanno fornito preziosi suggerimenti.

IL SEGRETARIO

(A. M. Contessa)

INDICE

1. INTRODUZIONE

La sempre maggior diffusione di applicazioni *real-time* a supporto del *core business* aziendale ha aumentato la necessità che, per garantire la disponibilità e l'efficienza dei servizi offerti, venga assicurata la continuità di servizio di alcune parti del sistema informatico. Queste ultime, cosiddette "vitali", variano ovviamente, da impresa a impresa, a seconda delle relative caratteristiche. Per le aziende è di importanza strategica assicurarne l'operatività e individuare opportune misure di emergenza, in caso di malfunzionamento o indisponibilità.

Questo documento ha l'obiettivo di fornire una metodologia di analisi e un insieme di regole di comportamento, descritte anche mediante "analisi di casi", che possano costituire un punto di riferimento utile per le aziende del sistema bancario. Esso è diretto ai responsabili di progetto di applicazioni vitali e ai *team* che si occupano della gestione dell'emergenza, compresi gli utenti. Esso può costituire anche un utile strumento per la Direzione, chiamata a decidere sull'attuazione dei vari progetti e ad assumersi le responsabilità dei "rischi residui" che le varie scelte comportano.

Nella prima parte sono trattate le problematiche relative alla continuità di servizio, nella seconda quelle attinenti alla gestione dell'emergenza. In appendice viene riportata una metodologia che consente di individuare, attraverso un'opportuna analisi del rischio, le applicazioni vitali.

2. COME GARANTIRE LA CONTINUITÀ DI SERVIZIO

La continuità di servizio è uno dei parametri fondamentali da considerare in sede di progettazione di una data applicazione: nel corso dell'analisi dei rischi gli utenti all'interno dell'azienda devono individuare le conseguenze di malfunzionamenti e fermi in tutte le possibili condizioni operative. In questo documento saranno considerate solo le applicazioni vitali, per le quali il livello di rischio di conseguenze particolarmente negative associato all'indisponibilità è "alto" (cfr. Appendice).

Per esse si forniranno indicazioni e accorgimenti atti a ridurre al minimo tale rischio. Fra le possibili cause si esamineranno non solo guasti a impianti, sistemi e reti e malfunzionamenti software, ma anche errori operativi e la necessità di manutenzione ordinaria e straordinaria. Quest'ultimo aspetto assume oggi importanza rilevante con la diffusione su Internet di servizi per la clientela operativi per tutto l'arco delle ventiquattro ore.

Va sottolineato che carenze nella fase progettuale che non tengono nel dovuto conto le esigenze di continuità di servizio si riflettono in disservizi in produzione. Inoltre, le applicazioni vitali necessitano di una gestione attenta, mirata a prevenire l'insorgere di problemi ed eventualmente a risolverli, contenendo al minimo i tempi di fermo. Nel seguito sono illustrate entrambe le fasi.

2.1 NELLE FASI PROGETTUALI

La progettazione del sistema informatico e logistico in cui collocare una applicazione vitale e lo sviluppo di quest'ultima usualmente seguono le stesse metodologie e fasi adottate per tutte le altre applicazioni. Gli aspetti peculiari, illustrati in dettaglio di seguito, sono rinvenibili in un più elevato livello di ridondanza delle componenti e in una maggiore attenzione alle tecniche di sviluppo e di sicurezza direttamente connessi alla continuità di servizio.

2.1.1 Ridondanza

Il sistema informatico e logistico deve avere caratteristiche di alta disponibilità per garantire il ripristino delle funzionalità a fronte di qualunque tipo di guasto nei tempi massimi stabiliti. La ridondanza consente di ridurre il numero di componenti la cui indisponibilità comporta quella dell'applicazione vitale. Occorre progettare impianti, sistemi e reti individuando tutti i possibili singoli punti di guasto e, ove possibile, eliminandoli ricorrendo a duplicazioni. Lo *switch* da una componente a quella duplicata deve avvenire in caso di necessità, in modalità manuale o automatica, con il minor disservizio possibile per gli utenti dell'applicazione. Caso limite è quello dei sistemi *fault tolerant* che non hanno *single point of failure* e, in presenza di un guasto singolo, sono in grado automaticamente e senza tempi di fermo di commutare dalla componente guasta a quella duplicata.

Poiché le componenti di un ambiente ad alta disponibilità richiedono, come qualunque altro ambiente, interventi di manutenzione ordinaria e straordinaria, la ridondanza può anche essere utilizzata per ridurre o annullare i necessari tempi di fermo. Questo è, ad esempio, cruciale nei sistemi in cui l'applicazione vitale deve essere operativa tutto l'anno, ventiquattro ore al giorno.

La ridondanza è costosa; tuttavia, in sua assenza, i costi di fermo applicativo e di gestione rischiano di divenire elevatissimi; inoltre, non è certo che i tempi massimi di ripristino possano essere rispettati (ad esempio, senza sito di disaster recovery in caso di disastro non è possibile ripartire in tempi brevi).

2.1.1.1 Impianti

La prima forma di ridondanza nei sistemi di elaborazione dati è stata storicamente introdotta per gli impianti di alimentazione, che possono essere duplicati: i) ricorrendo all'autoproduzione per la seconda fonte, ad esempio mediante l'utilizzo di sistemi a turbina alimentati a gasolio; ii) chiedendo al fornitore di energia due distinte consegne in media tensione, iii) ricorrendo a due diversi fornitori. I due sistemi alternativi di alimentazione vengono convogliati su gruppi di batterie (UPS) in grado di alimentare il centro in assenza di entrambe le fonti per un periodo di tempo limitato, normalmente non più di qualche decina di minuti. In caso di caduta di alimentazione e all'interno di tale intervallo di tempo deve essere effettuato lo *switch* automatico da un sistema all'altro, attraverso un sistema di controllo e verifica della tensione di alimentazione che pilota, in caso di autoproduzione, anche l'accensione delle turbine. Nel caso di sistemi intermedi e apparati di rete distribuiti su più stabili, in cui non è possibile o troppo costoso ricorrere a due fonti distinte di alimentazione, si dovrà disporre di UPS *ad hoc*, di caratteristiche adeguate a garantire autonomia a fronte di prolungate sospensioni dell'erogazione di energia elettrica.

La ridondanza deve ovviamente riguardare tutta la catena di distribuzione fino all'alimentazione degli apparati del sistema informatico e, in particolare, dei quadri elettrici centrali e locali e delle linee di distribuzione.

Infine, relativamente agli impianti di condizionamento, è opportuno prevedere un sovradimensionamento o una ridondanza tale da garantire il condizionamento dei sistemi a fronte di guasti e manutenzione.

2.1.1.2 Hardware

Gli elaboratori centrali (*mainframe*) sono prodotti con elevati livelli di ridondanza; sono ridondati i processori, i canali di collegamento verso le unità di controllo, i sistemi di alimentazione dei dispositivi, le linee di raffreddamento, i banchi di memoria, ecc. Negli elaboratori di ultima generazione sono addirittura previsti processori di riserva, normalmente non utilizzati, in grado di sostituirsi a processori guasti in modo dinamico. Anche gli elaboratori intermedi (elaboratori AS/400, server UNIX e Windows/NT ecc.), seppure in grado minore, presentano livelli di ridondanza e spesso consentono attraverso tecniche di *clustering* di sopperire al fermo di un sistema.

La ridondanza dei dischi magnetici è oggi garantita dall'architettura RAID attraverso la duplicazione completa dei dati (RAID1, *mirroring*), ovvero attraverso tecniche più sofisticate basate su algoritmi di parità finalizzate a ridurre lo spazio complessivamente necessario per la ridondanza

(RAID4, RAID5). Nei sottosistemi di memorizzazione sono sempre previsti dischi di riserva che si sostituiscono dinamicamente a un disco guasto il cui contenuto viene ripristinato in modo automatico e trasparente. Sulle unità nastro la ridondanza è garantita dalla disponibilità di più supporti e quindi dalla duplicazione fisica delle informazioni su due supporti diversi.

Di fronte a tutte queste possibilità è compito dei progettisti valutare fin dove spingersi, in base ai requisiti di continuità di servizio richiesti dall'applicazione vitale. Vincoli architetturali potrebbero essere posti dall'applicazione medesima, specie nel caso si dovesse ricorrere a pacchetti disponibili solo per specifici sistemi intermedi. L'eventualità di una tale occorrenza dovrebbe peraltro essere limitata a casi veramente eccezionali.

Opportuni accorgimenti "a basso costo" possono consentire miglioramenti notevoli per quanto riguarda la disponibilità a fronte di guasti e di manutenzione, ad esempio attraverso il collegamento delle doppie alimentazioni a quadri elettrici distinti e delle doppie schede di rete ad apparati nodali distinti, qualora i quadri elettrici e gli apparati nodali siano ridondati.

2.1.1.3 Infrastruttura di rete

I problemi che possono causare l'interruzione del traffico su una rete di comunicazione sono i malfunzionamenti e i guasti che interessano i nodi di partenza, le linee di comunicazione, i nodi intermedi e i nodi di arrivo. Per eliminarne o limitarne le conseguenze, tutte le componenti che realizzano un percorso fisico (apparati nodali e linee) dovrebbero essere duplicate e, nel caso di siti distinti, dovrebbero essere previsti percorsi fisicamente distinti. Le comunicazioni principali e quelle di *backup* possono essere realizzate con tecnologie differenti (ad esempio su rete satellitare e terrestre). Se possibile, le apparecchiature e le linee di riserva andrebbero predisposte in modo da consentirne l'utilizzo anche durante la normale operatività, affinché guasti e attività di manutenzione non compromettano la continuità di servizio delle applicazioni vitali. È consigliabile l'adozione di architetture di rete e protocolli standard per la gestione in modalità automatica delle ridondanze degli apparati nodali (*router, switch, hub*) e della diversificazione degli instradamenti.

2.1.1.4 Software

In ambienti ad altissima criticità, ad esempio nei progetti spaziali, ove il fermo della elaborazione può comportare rischi alla vita umana, la ridondanza è applicata alle componenti *hardware* in misura più estesa (ridondanza tripla, quadrupla o maggiore) ed è anche applicata alle componenti *software* di base e applicative che sono duplicate e, per evitare lo stesso errore sulle copie, queste sono realizzate, con le stesse funzionalità, da fornitori diversi.

In ambienti elaborativi dedicati ad applicazioni commerciali, quali quelle bancarie, la ridondanza è applicata alle sole componenti hardware. È possibile che il software di base e applicativo sia presente in più copie su diverse regioni indipendenti di un medesimo elaboratore o su più elaboratori; gli eventuali errori software si manifesteranno però in tutte le copie disponibili e porteranno al fermo delle applicazioni interessate o, in situazioni più gravi, a errori nell'elaborazione dei dati.

Obiettivi perseguibili con più copie dello stesso *software,* a prescindere dagli errori, sono quelli di consentire un miglior bilanciamento del carico elaborativo e la gestione, la manutenzione e l'aggiornamento del *software* di base e applicativo senza interruzione di servizio, aspetti anch'essi di particolare interesse per le applicazioni vitali a disponibilità continua. Nel caso dei sistemi

centrali può ad esempio essere utilizzata a tale scopo la tecnologia Parallel Sysplex che consente, con l'ausilio di funzioni avanzate del sistema operativo recentemente introdotte, di interrompere l'esecuzione delle applicazioni su un elaboratore che fa parte del complesso e di continuarla su un altro.

Per le sole applicazioni vitali, per fronteggiare malfunzionamenti e guasti al sistema informatico e, quindi, anche errori *software*, è consigliabile lo sviluppo di moduli aggiuntivi semplificati, da installare su elaboratori dipartimentali o *personal computer* presso gli utenti delle applicazioni medesime, che consentano di garantire una operatività minima, compatibile con la prosecuzione del *business* aziendale.

2.1.1.5 Dati

Una prima e fondamentale ridondanza dei dati consiste nel mantenere copie di riserva degli ambienti applicativi e degli archivi utilizzati dalle applicazioni vitali, eseguite con periodicità prestabilita, per permettere la ripresa delle elaborazioni in caso di perdita di uno o più di essi. Sono oggi disponibili sottosistemi che consentono di effettuare in parallelo due o più copie su supporti di memorizzazione di secondo livello nello stesso sito o in siti remoti.

Per garantire l'integrità dei dati e la continuità delle elaborazioni a fronte di un singolo errore su disco, si usano tecniche automatiche di ridondanza in tempo reale di tipo RAID (cfr. par. 2.1.1.2).

Altra tecnologia di ridondanza automatica ampiamente diffusa è quella della cosiddetta copia remota sincrona. La copia dei dati è eseguita in tempo reale in un sito remoto rispetto a quello principale e consente, in caso di *disaster recovery*, di far ripartire le applicazioni con i dati allineati all'ultimo aggiornamento effettuato prima del fermo.

2.1.1.6 Centri elaborazione dati

Per consentire alle applicazioni vitali di ripartire in caso di indisponibilità del sito principale è necessario disporre di un sito alternativo. La duplicazione del CED può consentire di effettuare *recovery* parziali e totali e, a seconda dei requisiti di continuità di servizio richiesti, può essere realizzata in ambiente aziendale o presso un fornitore di servizi, con diverse modalità.

Una prima soluzione, detta *empty shell*, prevede l'allestimento in un sito remoto dei soli impianti elettrici e di condizionamento e l'attestazione delle connessioni di rete. Gli elaboratori necessari saranno installati da un fornitore di servizi solo a fronte di una situazione di *disaster recovery*. Copie degli ambienti applicativi e degli archivi necessari per riattivare le applicazioni saranno trasferite periodicamente nel sito secondario e ivi conservate. Una variante a questa prima soluzione prevede la presenza di elaboratori non operativi nel sito secondario, i cui dati sono aggiornati periodicamente con modalità fuori linea (trasferimento di supporti magnetici o copie remote via linea trasmissione dati). Soluzioni di questo tipo prevedono tempi di ripristino elevati, dell'ordine di qualche giorno, e richiedono la predisposizione di apposite e complesse procedure organizzative.

Una soluzione intermedia prevede l'installazione di elaboratori anche nel sito secondario, da utilizzare per altre applicazioni, così da suddividere il carico fra i due centri, e l'utilizzo della

tecnica della copia remota sincrona dei dati. Questa soluzione prevede tempi di ripristino limitato, dell'ordine di qualche ora e la predisposizione di semplici procedure organizzative.

La soluzione più avanzata prevede che in caso di fermo del sito primario il sistema remoto in *stand-by* sia in grado di prendere il controllo delle operazioni e di proseguire l'attività in assenza o con un minimo di intervento operativo. Un'architettura che oggi offre tale soluzione per i *mainframe* è quella del *Geographically Dispersed Parallel Sysplex*; per diversi sistemi intermedi esiste una configurazione analoga detta di *clustering* remoto. Entrambe queste soluzioni sono realizzabili purché la distanza fra i due siti sia limitata (al massimo 10-20 chilometri).

A seconda delle necessità sono possibili anche altre soluzioni che si collocano in una posizione intermedia fra quelle indicate; i costi possono variare notevolmente a seconda delle soluzioni e normalmente crescono al ridursi dei tempi necessari al ripristino dell'operatività nel sito secondario.

2.1.2 Modalità di sviluppo

Ogni azienda dovrebbe essere dotata di un sistema di qualità, atto a certificare l'intero processo di sviluppo e non solo il prodotto finale. La necessità di un sistema di qualità aumenta se, come spesso avviene, si ricorre a società esterne per le fasi di progettazione, scrittura e manutenzione del codice di un'applicazione o per l'acquisizione e la personalizzazione di pacchetti.

Nel caso di applicazioni vitali occorre inoltre adottare tutti gli accorgimenti che, in caso di problemi, agevolano l'individuazione delle componenti software in errore, il ripristino della funzionalità e consentono di ridurre al minimo i danni dovuti a malfunzionamenti o fermi di componenti della stessa o di altre applicazioni. Ad esempio, nel caso delle procedure operative e contabili tipiche del settore bancario, dovrebbero essere realizzati moduli applicativi *ad hoc* per il controllo del corretto allineamento delle informazioni anagrafiche e delle quadrature contabili sia nelle singole procedure sia fra procedure diverse.

Attenzione particolare dovrebbe anche essere dedicata al disegno dell'architettura complessiva dell'applicazione vitale, affinché le usuali operazioni di gestione non abbiano impatto sulla continuità di servizio. Ad esempio un obiettivo potrebbe essere quello di ridurre il più possibile le fasi di *batch* serale e di renderle non condizionanti per l'avvio della giornata operativa. Per quanto riguarda le basi dati, le tecnologie *hardware* e *software* disponibili consentono già oggi di ridurre sensibilmente le esigenze di fermo, rendendo possibili l'esecuzione di *backup* e *image copy* anche durante la giornata operativa. Un buon disegno delle basi dati rimane ovviamente cruciale per ottenere adeguati tempi di risposta e quindi, indirettamente, una buona continuità di servizio per l'applicazione vitale.

2.1.2.1 Modularità

Questa tecnica di sviluppo, elaborata da oltre un ventennio, se utilizzata propriamente consente una gestione più semplice e veloce degli errori *software.* Infatti, la suddivisione del codice in moduli agevola l'individuazione e la correzione delle componenti in errore.

2.1.2.2 Indipendenza

Quanto più un'applicazione è indipendente dalle altre che operano in uno stesso sistema informatico, tanto più è limitata la possibilità di propagazione di errori *software*. Nel caso delle applicazioni vitali tale disaccoppiamento è rafforzato utilizzando tecniche di colloquio asincrono; in tal modo è possibile garantire la funzionalità di un'applicazione vitale per periodi di tempo sufficientemente lunghi anche qualora altre applicazioni non siano operative.

In talune circostanze, per garantire la massima stabilità ambientale può essere consigliabile arrivare a forme di isolamento logico o fisico: verrà utilizzato un ambiente o un intero elaboratore ad alta disponibiltà per una sola o poche applicazioni vitali fra loro fortemente connesse.

2.1.2.3 Test

La progettazione, la pianificazione, l'esecuzione, la verifica e validazione dei test, importanti in qualunque attività di sviluppo, diventano una fase cruciale nello sviluppo di una applicazione vitale. Tali attività dovrebbero essere svolte da un gruppo distinto da quello che segue le altre fasi del progetto e coinvolgere gli utenti. Anche se tali attività sono affidate a una ditta esterna, il controllo da parte di personale dell'azienda dovrebbe essere continuo e il più possibile stringente, per verificare che la copertura assicurata dai test sia la più ampia possibile. Si ricorda che per le applicazioni vitali, normalmente, i costi da sostenere per le fasi di test sono comparabili a quelli di tutte le altre fasi del progetto di sviluppo.

2.1.2.4 Documentazione

La documentazione è importante in tutte le attività di sviluppo e quindi, a maggior ragione, dovrà esserne curata la completezza e la qualità nel caso delle applicazioni vitali. Per queste ultime, inoltre, particolare attenzione dovrà essere posta a quella per il *problem management*: i messaggi di errore forniti a programma devono essere il più possibili chiari e autoesplicativi e a fronte di ogni anomalia deve essere prevista una documentazione sintetica a disposizione dei presidi operativi (*help desk* e specialisti), per consentire con la massima tempestività e sicurezza eventuali interventi sul codice o sui dati.

2.1.2.5 Controllo qualità

Il controllo qualità può essere un ulteriore incentivo a fare le cose bene, in quanto vincola l'utente a definire in modo quantitativo i requisiti di qualità richiesti dall'applicazione vitale (affidabilità, robustezza, integrità, manutenibilità, gestibilità, ecc.) e quindi, in particolare, quelli di continuità di servizio e il fornitore a rispettarli. È normalmente molto costoso.

Il controllo qualità dovrebbe coprire l'intero processo di sviluppo, quindi anche le fasi di test e di produzione della documentazione precedentemente descritte, ed essere svolto a cadenza preordinata durante lo svolgimento delle varie fasi di progettazione o per lo meno prima dell'avvio

in produzione dell'applicazione vitale. È sconsigliabile effettuarlo *ex post*, dopo l'avvio dell'attività operativa.

2.1.3 Aspetti di sicurezza

La sicurezza fisica e logica delle infrastrutture informatiche ha l'obiettivo di garantire condizioni che consentano adeguati livelli di integrità, riservatezza e disponibilità delle applicazioni e delle informazioni. Essa è pertanto condizione essenziale per la continuità di servizio[1]. Nel caso di applicazioni vitali occorre evitare, in fase progettuale, di indebolire il sistema di sicurezza esistente e, se necessario, rafforzarlo ulteriormente.

Per quanto riguarda la sicurezza fisica occorre verificare che le aree contenenti le componenti del sistema informatico siano classificate e adeguatamente protette oppure procedere in tale senso. Attenzione dovrebbe essere dedicata anche alle possibili misure tecniche e organizzative atte a ridurre il più possibile le cause di errore operativo nell'azionamento di impianti e sistemi (ad esempio doppi interruttori e regola dei "quattro occhi"), che sono spesso causa di fermi delle applicazioni vitali e che sono ben più probabili di eventi dolosi o fraudolenti. Dovrebbero essere adibiti locali protetti e a prova di incendio, se possibile in stabili differenti, alla conservazione di copie dei dati e delle applicazioni medesime.

Per quanto attiene la sicurezza logica, è necessario prevedere una adeguata protezione dei dati, delle applicazioni medesime e dei canali di trasmissione mediante tecniche di autenticazione e di crittografia e, nel caso di connessioni a reti esterne, di separazione che prevedono l'interposizione di dispositivi *router* e *firewall* e, in casi estremi, la mancanza di una connessione diretta. Anche nel caso della sicurezza logica particolare attenzione andrebbe posta alle misure tecniche e organizzative atte a ridurre le cause di errore operativo.

Infine, dovrebbe essere valutata l'adeguatezza dei meccanismi utilizzati per tracciare e memorizzare gli eventi anomali, che potrebbero indicare una situazione di rischio per la sicurezza. Nei casi potenzialmente più critici sarebbe anche opportuno inserire dei meccanismi di allarme che li segnalino in tempo reale.

2.2 NELLA GESTIONE CORRENTE

La gestione corrente delle applicazioni vitali è inserita nel contesto della gestione dei sistemi informatici e logistici in cui sono collocate e che normalmente condividono con altre applicazioni. Dovendo garantire stringenti requisiti di continuità di servizio è indispensabile conoscere momento per momento lo stato di funzionamento di questi sistemi, monitorando le risorse critiche e i margini di riserva. È altresì essenziale ricorrere, ove possibile, all'automazione e al controllo operativo per tutte le operazioni di gestione corrente, al fine di utilizzare al meglio le risorse, ridurre la possibilità

[1] È necessario che la sicurezza informatica abbia la medesima considerazione di quella riservata alle infrastrutture di protezione dei valori. Ogni azienda dovrebbe avere le proprie norme e standard di sicurezza informatica. La sicurezza informatica dovrebbe essere considerata un problema aziendale e non solo del dipartimento informatico.

di errore operativo e far pervenire tempestivamente segnali di allarme non solo per le componenti impiantistiche e di sistema, ma anche per quelle dell'applicazione vitale in esame (errori applicativi bloccanti).

Rimane centrale l'importanza dei presidi operativi, che devono essere in grado di operare in modo proattivo a fronte di scostamenti dal normale stato di funzionamento e in modo reattivo a fronte di anomalie o errori che possono comportare malfunzionamenti o fermi all'applicazione vitale. La struttura dei presidi deve tener conto che per le applicazioni di tipo distribuito il confine tra componenti applicative, di sistema e di rete è sempre più labile. Devono quindi essere il più possibile unificati e ricorrere a *tool* di *management* integrati.

Particolare attenzione deve essere posta alle modifiche ai sistemi, alla rete e al software di base e applicativo. Riunioni periodiche coordinate da un responsabile tecnico dovrebbero presiedere la gestione delle modifiche.

Dovrebbero essere previsti *report* per la Direzione nel caso di scostamenti rispetto ai livelli di continuità di servizio richiesti dall'applicazione vitale ed, eventualmente, l'attivazione di meccanismi di *audit*.

2.2.1 Risorse critiche e accessorie

Un sistema ad alta disponibilità deve essere in grado di funzionare per periodi di tempo relativamente lunghi, una o più giornate operative, senza interventi da parte degli operatori.

L'autonomia si ottiene non solo facendo ricorso a opportune forme di ridondanza e a un corretto dimensionamento delle risorse *hardware* critiche e accessorie in fase di progetto, ma anche con la corretta gestione di queste ultime. Occorre effettuare un monitoraggio attento delle risorse critiche e dei margini di riserva e provvedere per tempo a fronte di possibili saturazioni.

L'attività di *capacity planning* consentirà di individuare a medio termine l'ammontare di risorse necessarie per garantire adeguati margini di riserva; attraverso l'automazione e il controllo operativi sarà invece possibile calibrare le risorse per fronteggiare le situazioni momento per momento.

2.2.2 Automazione operativa

Con il termine automazione operativa si intende l'utilizzo di componenti *software* e *hardware* per lo svolgimento delle attività necessarie al corretto funzionamento del sistema informatico: attivazione e disattivazione dei sistemi, delle reti e delle applicazioni, controllo dello stato delle risorse, gestione dei carichi di lavoro e così via.

Un alto livello di automazione aumenta la disponibilità dei sistemi e delle applicazioni perché diminuisce gli errori umani e garantisce che, a fronte delle medesime condizioni operative, vengano eseguite sempre le stesse procedure. Le modalità con cui l'automazione interagisce con il sistema devono essere definite da opportune politiche di gestione; tali politiche devono essere codificate in appositi *file* di configurazione, facilmente modificabili dal personale tecnico abilitato.

L'automazione deve effettuare con continuità il monitoraggio della funzionalità di tutte le risorse necessarie alla fornitura del servizio applicativo, segnalando all'operatore le eventuali anomalie. Per ogni componente le grandezze da controllare vanno decise con attenzione; va tenuto

conto, infatti, che, rispetto alla funzionalità del servizio applicativo, la semplice disponibilità di una risorsa non è sufficiente; infatti, una risorsa può risultare disponibile, ma non utilizzabile, ad esempio perché ha delle performance inadeguate o perché viene interdetta, nel suo funzionamento, da politiche di sicurezza errate.

L'automazione, oltre a tutte le condizioni di normale operatività, dovrebbe gestire anche i malfunzionamenti più comuni e assistere l'operatore nella gestione dei malfunzionamenti più gravi o meno frequenti. Il confine tra le condizioni che devono essere gestite automaticamente e quelle che devono essere lasciate alla decisione dell'operatore va tracciato tenendo conto di diversi fattori, quali la gravità del malfunzionamento e il rapporto costo/beneficio nello sviluppo di procedure per la gestione di errori poco frequenti. Va ricordato che le procedure di automazione devono essere "robuste" e quindi il più possibile semplici in quanto normalmente non sono soggette a loro volta a controllo.

Nel caso di errori, l'automazione dovrebbe presentare all'operatore solamente le segnalazioni importanti, evitando le duplicazioni e filtrando quelle non necessarie; può essere utile presentare all'operatore delle possibili opzioni tra le quali scegliere quella migliore nella particolare condizione. In ogni caso l'intero processo decisionale, che richiede analisi di situazioni complesse e la scelta tra più opzioni, non può essere automatizzato.

2.2.3 Controllo operativo

Con il termine controllo operativo si intende la parte di gestione che è affidata al diretto intervento dell'operatore; in un ambiente con una automazione operativa fortemente sviluppata, tale intervento dovrebbe essere limitato alla gestione delle condizioni di errore o di degrado del servizio.

Le condizioni di perdita o di degrado dell'operatività devono essere rilevate al più presto, in modo automatico, con l'obiettivo di far intervenire le funzioni di assistenza prima della segnalazione di problemi da parte dell'utente; le relative segnalazioni di allarme devono essere presentate nel modo più chiaro possibile e devono essere inviate, a seconda dei casi, con diverse modalità (icone colorate su una interfaccia grafica, messaggi a console, chiamate a un *teledrin pager*).

La funzionalità della catena di componenti (*hardware*, *software* e di rete) che trasporta gli allarmi dalla periferia ai sistemi di raccolta e di segnalazione, deve essere il più possibile affidabile e comunque tenuta costantemente sotto controllo (tipicamente, con allarmi di *heartbeat*).

Per ogni allarme deve essere disponibile una documentazione di dettaglio, che riporti il significato dell'allarme, le procedure di ripristino o di *bypass* e la funzione di supporto a cui scalare eventualmente il problema. Nel caso in cui i diversi livelli di supporto non abbiano provveduto a risolvere o a scalare il problema entro un tempo prefissato, può essere utile prevedere meccanismi di *escalation* automatici.

Dovrebbe essere posta massima attenzione, oltre che alla tradizionale gestione delle risorse di sistema, degli apparati di rete e dei sistemi di gestione di basi di dati, alla gestione delle applicazioni vitali medesime; spesso, specialmente nei sistemi *client/server*, le applicazioni si bloccano senza segnalazioni e senza che gli operatori conoscano le procedure di ripristino.

All’operatore dovrebbe essere fornita, per il controllo delle risorse e per l’esecuzione dei comandi, una interfaccia unica e indipendente dalle varie piattaforme; inoltre, per le condizioni di errore complesse, dovrebbero essere resi disponibili strumenti di ausilio alla determinazione delle cause del problema (*tool* di analisi, accesso agli archivi dei problemi che si sono già verificati).

2.2.4 Sicurezza

Nella gestione corrente occorre un controllo puntuale e continuo di tutto ciò che concerne la sicurezza. Anche un buon sistema di protezione può infatti fallire se è male utilizzato o disatteso. Occorre quindi che siano applicate le misure di sicurezza stabilite e che ne sia verificata l’effettiva applicazione. Particolare cura andrà riservata agli aspetti normativi e organizzativi e alla sensibilizzazione di tutto il personale, con particolare riferimento al corretto trattamento delle informazioni riservate (*password* personali di accesso, chiavi crittografiche, ecc.).

Per quanto riguarda la sicurezza fisica, oltre al collaudo periodico di eventuali impianti di sicurezza, dovrebbe essere controllato l’accesso alle aree protette e tenuta aggiornata la lista del personale interno ed esterno abilitato. Le copie di *backup* dei dati, effettuate a cadenza prestabilita, e del codice delle applicazioni vitali dopo ogni modifica dovrebbero essere collocate in appositi locali protetti e a prova di incendio.

Per quanto riguarda la sicurezza logica, analoga cura dovrà essere posta all’accesso ai sistemi e alle reti utilizzati dalle applicazioni vitali, ai loro dati e alle applicazioni medesime. Ai dati, in particolare, si dovrebbe accedere esclusivamente attraverso le sole applicazioni: non dovrebbe essere prevista alcuna autorizzazione permanente di accesso diretto ai dati; gli interventi di natura sistemistica e applicativa dovrebbero essere effettuati utilizzando apposite utenze, dotate degli opportuni privilegi e autorizzazione di accesso. Dato il potenziale distruttivo e la capacità di diffusione dei virus informatici, dovrebbero essere previste procedure di controllo dei supporti informatici ricevuti dall’esterno, inclusi dati e messaggi scambiati via posta elettronica.

Tutte le situazioni con potenziali rischi di sicurezza, sia fisica sia logica, dovrebbero essere tracciate e controllate da un opportuno presidio di sicurezza e *report* periodici dovrebbero essere trasmessi a funzioni di *audit* interno. La verifica periodica dell’efficacia delle misure di protezione adottate potrà comportare revisioni alle stesse e quindi l’avvio di una specifica attività di gestione o di un progetto di adeguamento.

2.2.5 Presidi operativi e gestione del personale

La gestione di sistemi ad alta disponibilità richiede la presenza di diversi specialisti qualificati. Da un lato, infatti, i compiti e le conoscenze richieste sono assai diversificati a seconda della componente del sistema informatico da gestire e controllare, dall’altro i tempi di reazione e di soluzione di eventuali problemi devono essere il più possibile brevi. Per contro, gli utenti delle applicazioni vorrebbero avere sempre un unico referente, qualunque sia il problema da risolvere, senza tenere conto dei confini tra componenti applicative, di sistema e di rete.

La soluzione normalmente adottata, anche per contenere i costi, è quella di un unico presidio operativo su più livelli. Il primo, con funzioni di *help desk*, è utilizzato per tutte le strutture informatiche dell’azienda e, dovendo essere attivo in tutto l’arco della giornata in cui vi sono applicazioni vitali funzionanti, opera di norma su turni. L’*help desk* ha i compiti propri del controllo

operativo relativi alla gestione delle condizioni di errore e di degrado dell'operatività segnalati dagli strumenti di automazione operativa o direttamente dall'utenza interna ed esterna. In particolare svolge il ruolo di interfaccia unico con l'utenza per le richieste di supporto, le segnalazioni di problemi e gli eventuali reclami. È cruciale che siano stabilite delle priorità e dei tempi massimi di intervento nonché delle modalità di *escalation* per tutti i problemi che possono ripercuotersi sulla continuità di servizio delle applicazioni vitali.

I livelli di presidio successivi hanno carattere specialistico e coprono tutte le aree tecniche necessarie: impiantistiche, sistemistiche, di rete, applicative e di sicurezza, e sono di norma disponibili in orario di ufficio presso le unità tecniche di appartenenza e, al di fuori di esso, in reperibilità. Compito dei livelli di presidio successivi è quello di subentrare agli operatori dell'*help desk* per la soluzione dei problemi più complessi; la loro attivazione avviene di norma su richiesta dell'*help desk* medesimo e, al di fuori degli orari in cui quest'ultimo è presente, mediante allarmi inviati dagli strumenti di automazione operativa. A seconda della realtà aziendale, i livelli di presidio successivi possono essere uno o due. Se due, il primo di questi dovrebbe essere visto come *back office* dell'*help desk* e operare in stretto contatto con esso.

Nel caso di applicazioni vitali, per aumentare l'efficacia degli interventi, è possibile inviare allarmi in parallelo all'*help desk* e a presidi di livello superiore ed, eventualmente, richiedere la presenza presso l'*help desk* stesso di alcuni specialisti nei momenti più critici della giornata operativa, ad esempio nelle fasi di apertura e chiusura e in prossimità di particolari *cut off.*

Fra i compiti del presidio operativo dovrebbe anche esserci quello di conservare le informazioni relative a tutti i problemi trattati, dall'apertura alla chiusura, e alle soluzioni adottate. L'*help desk* potrebbe occuparsi di tutto il processo con la sola eccezione della descrizione della soluzione quando questa è stata curata dai livelli di presidio successivi. In presenza di un secondo livello di *back office,* a quest'ultimo potrebbe essere delegato il compito di verifica e completamento della documentazione relativa a tutti i problemi trattati e la loro chiusura. Per svolgere al meglio questa attività sarebbe auspicabile l'adozione di un idoneo *tool* di *management* integrato fra i tanti disponibili sul mercato.

Per quanto riguarda la gestione del personale, si ricorda che l'attività di presidio è particolarmente logorante. Occorrerebbe quindi prevedere opportune rotazioni di personale e percorsi di addestramento e riqualificazione. È possibile anche ricorrere per le funzioni di *help desk* e per alcune figure specialistiche di presidio operativo a forme più o meno intense di *outsourcing*.

2.2.6 Gestione delle modifiche

I sistemi ad alta disponibilità, come qualunque sistema informatico, sono soggetti a frequenti interventi di manutenzione e aggiornamento alle componenti impiantistiche, di rete, *hardware* e *software*. Possono inoltre essere necessarie temporanee variazioni di configurazione per l'esecuzione di prove di *recovery* locale e in siti remoti. Una pianificazione puntuale di tali attività è necessaria per garantire stabilità ai sistemi e quindi alle applicazioni vitali.

Il *change management* dovrebbe essere coordinato da un responsabile tecnico e la pianificazione dovrebbe essere fatta sulla base di incontri periodici con tutte le aree tecniche e con rappresentanti degli utenti, nei quali definire tempi e modalità dei singoli interventi, cercando di circoscriverne il più possibile gli impatti sulle altri componenti del sistema e senza entrare in conflitto con le esigenze di continuità di servizio degli utenti. Poiché tali attività devono essere fatte

normalmente al di fuori dell'orario di operatività e quindi, prevalentemente, nei fine settimana, la periodicità degli incontri dovrebbe essere almeno settimanale.

Le attività concordate e le relative implicazioni dovrebbero essere riportate in un apposito verbale, da distribuire a tutte le aree tecniche e agli utenti delle applicazioni vitali interessate, nonché ai *team* coinvolti nel *business contingency plan (BCP)*, per essere pronti ad attivare le misure di emergenza che si rendessero necessarie a fronte di effetti non previsti (cfr. capitolo 3).

Ovviamente tutte le modifiche di sistema, incluse quelle alla rete, e le modifiche applicative, coinvolgendo applicazioni vitali, dovrebbero essere provate in opportuni ambienti di test e solo successivamente propagate all'ambiente di produzione, garantendo sempre, in ogni caso, la possibilità di tornare alla situazione precedente alla modifica. In particolare le modifiche *software* dovrebbero sempre essere propagate utilizzando strumenti automatici per la gestione della configurazione. Gli utenti delle applicazioni vitali dovrebbero svolgere attività di collaudo e validazione delle modifiche prima di considerare concluso l'intervento; potrebbe rendersi necessario un ciclo analogo a quello previsto per la fase di test nella progettazione (cfr. par. 2.1.2.3).

Non dovrebbero essere consentite attività oltre a quelle stabilite nelle riunioni di *change management*, ad eccezione di quelle non programmabili e non procrastinabili a fronte di malfunzionamenti o guasti gravi che possono pregiudicare la funzionalità delle applicazioni vitali. Gli interventi di quest'ultimo tipo dovrebbero in ogni caso essere comunicati e verbalizzati nel corso della riunione di *change management* successiva.

2.2.7 Controllo interno ed esterno

L'adozione di adeguate procedure di controllo interno ed esterno rappresenta uno dei fattori chiave per garantire il mantenimento nel tempo di adeguati livelli di servizio in generale e di continuità di servizio in particolare.

Il controllo interno dovrebbe essere esteso a tutte le attività di gestione corrente trattate in questo capitolo, svolte sia dal personale interno sia da quello di ditte esterne. Su base periodica, dovrebbero essere raccolte a supporto opportune statistiche, atte a misurare non solo la quantità e l'efficacia degli interventi a fronte di anomalie, ma anche la qualità del servizio fornito all'utenza interna ed esterna dell'applicazione vitale.

Dovrebbero essere previsti r*eport* alla Direzione a fronte di scostamenti significativi della continuità di servizio rispetto a *target* predefiniti. Le statistiche e i *report* prodotti potrebbero consentire di individuare e adottare, se necessario, misure correttive di tipo tecnico e organizzativo.

Su base periodica, in linea con le direttive strategiche aziendali, le attività di gestione corrente potrebbero anche essere sottoposte a *audit* interno o esterno.

3. COME GESTIRE L'EMERGENZA

3.1 DEFINIZIONE DI SITUAZIONE DI EMERGENZA

Nonostante gli sforzi intrapresi per garantire la disponibilità e l'efficienza dei servizi offerti, può sempre capitare di dover fronteggiare situazioni di emergenza, dovute a fattori esterni o interni, che possono compromettere in parte o del tutto la funzionalità dei sistemi informatici aziendali.

Va ricordato che i rischi associati alle situazioni di emergenza relative alle applicazioni vitali dovrebbero essere noti a priori, in quanto identificati nell'ambito dell'analisi dei rischi nella fase iniziale della progettazione (cfr. Appendice).

Una possibile classificazione delle situazioni di emergenza, sulla base del livello di gravità, è la seguente:

- incidente: problema senza impatti per gli utenti interni ed esterni;
- incidente grave: problema con impatto solo nei confronti di utenti interni;
- situazione di crisi: problema con impatto anche nei confronti di utenti esterni;
- disastro: problema con impatti interni o esterni non risolvibile nei tempi di ripristino previsti.

3.2 BUSINESS CONTINGENCY PLAN

Per le varie tipologie di situazioni di emergenza sopra elencate vanno individuati: le possibili soluzioni, i team coinvolti, le strategie di coordinamento, le modalità di comunicazione interaziendali e con l'esterno. Ciò, nell'insieme, costituisce il Business Contingency Plan (BCP), che dovrebbe essere aggiornato ogni qual volta venga modificata una applicazione vitale o si intenda realizzarne una nuova. Affinché il BCP garantisca risultati soddisfacenti sono auspicabili, fra l'altro, l'esecuzione periodica di esercitazioni a tavolino e sul campo, nonché l'aggiornamento continuo delle strategie per tenere conto delle modifiche delle infrastrutture e del software di base e dell'esperienza acquisita nella gestione delle precedenti situazioni di emergenza.

Il BCP può anche essere realizzato a posteriori, relativamente ad applicazioni vitali già in produzione. Diverse aziende, ad esempio, ne hanno approntato uno "ad hoc" per poter gestire al meglio la transizione al nuovo millennio. Qualora un'azienda non avesse ancora un BCP e ritenesse vitale anche una sola applicazione, dovrebbe approntarne uno al più presto.

La modifica o realizzazione del BCP passa attraverso due fasi essenziali: lo sviluppo e la gestione. Di seguito vengono illustrate entrambe le fasi evidenziandone le peculiarità tecniche e organizzative.

3.2.1 Sviluppo del BCP

Nella fase di sviluppo di un'applicazione vitale, il BCP parte dall'esame di tutte le componenti del sistema informatico interessate, comprese le eventuali connessioni con sistemi e reti esterni all'azienda e implica:

- la descrizione analitica degli scenari di emergenza possibili;
- la definizione delle possibili soluzioni da adottare per ognuno di tali scenari;
- la definizione della struttura organizzativa preposta alla gestione dell'emergenza.

Al fine di individuare le soluzioni di emergenza, che nel caso di disastro devono avere carattere prevalentemente organizzativo, manuale o con basso contenuto di automazione, è necessario che l'utente dell'applicazione venga direttamente coinvolto. Successivamente, il piano deve essere approvato dalla Direzione. Le Aziende che si avvalgono di servizi forniti da terzi dovranno attivarsi per verificare lo stato di adeguamento dei loro piani di emergenza, anche per consentirne un'eventuale integrazione con quelli aziendali.

3.2.1.1 Scenari di emergenza

L'individuazione dei possibili scenari di emergenza, da effettuarsi congiuntamente da parte dei tecnici e degli utenti, dovrebbe partire dall'esame di come l'applicazione dovrà essere utilizzata, direttamente o indirettamente, dai diversi settori dell'azienda, tenendo conto degli impatti che deriverebbero dall'indisponibilità totale o parziale dell'applicazione stessa. Questi impatti dovrebbero essere stati precedentemente individuati dagli utenti nell'ambito dell'analisi dei rischi.

È poi necessario associare a ogni componente del sistema informatico e logistico utilizzato dall'applicazione (locali, impianti, sottosistemi *hardware*, infrastrutture di rete, componenti *software*) l'insieme degli eventi che possono causare un degrado prestazionale, un malfunzionamento oppure un blocco dell'applicazione. Questa associazione dovrebbe essere effettuata dai settori tecnici. Occorrerebbe anche tenere conto degli eventi che non hanno un impatto diretto sulla funzionalità dell'applicazione, ma possono ridurre l'affidabilità del sistema informatico dell'azienda, ad esempio nel caso di guasti di parti di impianto, di sistemi e reti ridondati.

Gli eventi che potrebbero compromettere la funzionalità possono essere classificati in vari modi; essi possono variare, entro certi limiti, a seconda del tipo dell'applicazione e dell'infrastruttura informatica e logistica in cui questa è collocata. Ad esempio, potrebbe essere dapprima seguita una classificazione di questo tipo: i) eventi esterni: mancanza di energia elettrica, indisponibilità di connessioni con eventuali sistemi e reti esterni all'azienda indispensabili alla funzionalità dell'applicazione, ecc.; ii) eventi interni: incendi, allagamenti, guasti agli impianti elettrici e di condizionamento, guasti ai sottosistemi *hardware* e agli apparati di rete, malfunzionamenti *software*, ecc.[2].

[2] Successivamente si potrebbe distinguere, all'interno delle due categorie, quelli di natura accidentale dovuti a cause naturali o a guasti o a errori operativi da quelli di origine dolosa, quali sabotaggio. Ovviamente, esiste la possibilità che un dato evento (ad esempio: l'incendio) possa essere di natura accidentale oppure dolosa.

L'incrocio fra componenti del sistema informatico e logistico utilizzato dall'applicazione ed eventi, ad esempio ricorrendo ad una tabella a doppia entrata, fornisce un quadro esaustivo dei possibili scenari di emergenza. Per comodità degli utenti sarebbe utile indicare, ove possibile, a fianco di ogni componente le parti di applicazione interessate. A questo punto è necessario che gli scenari di emergenza vengano ordinati in base al livello di gravità (incidente, incidente grave, situazione di crisi, disastro), tentando di associare ad ognuno una specifica probabilità di accadimento.

Qualunque sia lo scenario di emergenza, poiché si tratta di applicazioni vitali, è necessario individuare e contrattare con gli utenti i tempi massimi di ripristino, anche parziale, della funzionalità. Questi "tempi massimi" portano, se superati, al passaggio automatico a soluzioni di *contingency* estrema a cura degli utenti. All'interno del lasso di tempo disponibile, i tecnici possono porre in atto soluzioni già studiate e predisposte per eliminare il problema o superarlo ricorrendo a varie misure di *recovery,* di cui quella massima, quando prevista e per il solo caso di problemi di tipo infrastrutturale[3], è il *disaster recovery* in un sito secondario. Tali misure costituiscono, nel loro insieme, il *business continuity plan*, che indica tempi e modalità di ripristino della funzionalità dell'applicazione a seguito di una situazione di emergenza. Il *Business Contingency Plan* (BCP) considera, invece, anche le misure di *contingency* per far fronte all'impossibilità di garantire il ripristino nei tempi massimi previsti.

Affinché una situazione di emergenza venga individuata e correttamente inquadrata nei tempi più brevi possibili, è indispensabile che l'analisi degli "scenari di emergenza" sia la più chiara e semplice possibile e possa essere facilmente utilizzabile all'occorrenza anche da persone che non abbiano direttamente contribuito alla sua elaborazione.

3.2.1.2 Possibili soluzioni

Per ognuno degli scenari di emergenza individuati occorre stabilire le possibili soluzioni, tenendo conto dei tempi massimi di ripristino previsti[4]. Ogni soluzione deve essere corredata da una *checklist* che indichi per ogni passo: a) i *team* di tecnici o di utenti responsabili della esecuzione; b) le modalità di comunicazione fra i *team* interessati; c) i tempi di avvio e di completamento. La *checklist* deve inoltre prevedere il passaggio ad altre soluzioni, qualora quella adottata non fosse risolutiva. Infine, deve riportare i passi necessari a rientrare dalla situazione di emergenza a quella di normale funzionamento.

[3] Nel caso di malfunzionamenti software l'unica possibilità è, infatti, quella di individuarli ed eliminarli. Solo se i malfunzionamenti sono dovuti al rilascio di una nuova versione è possibile effettuare lo "switch" alla versione precedente.

[4] Particolare attenzione deve essere posta agli aspetti di sicurezza fisica e logica, infatti le situazioni di emergenza sono di difficile controllo e possono essere ideali per eventuali frodi. Per contro, i meccanismi di sicurezza adottati per la normale operatività potrebbero complicare la gestione dell'emergenza.

Si noti che le modalità e i tempi di *escalation* fra le diverse soluzioni di tipo tecnico e di tipo amministrativo dovrebbero essere definiti preventivamente all'interno della *checklist*. Quest'ultima dovrebbe essere verificata e certificata sul campo da gruppi di *auditor* interni o esterni.

Nel caso di incidenti a parti ridondate del sistema informatico e logistico e, più in generale, di quelli che non danno luogo a impatti per gli utenti, le soluzioni sono di natura tecnica. Trattandosi di problemi che riducono l'affidabilità di funzionamento dell'applicazione, la soluzione deve essere tempestiva ma, se possibile, eseguita al di fuori dell'orario di funzionamento, per non turbare l'ambiente operativo. Occorre in ogni caso comunicare alle aree tecniche e utente interessate l'esistenza di una situazione di preallarme, nonché tempi e modalità di ripristino.

Nel caso di incidenti gravi e di situazioni di crisi in cui ci sono impatti sull'operatività degli utenti, è necessario intervenire immediatamente con opportune misure tecniche che possono prevedere: riparazione del guasto; *recovery* a freddo di componenti *hardware* o di rete; rimozione di malfunzionamenti *software*; spostamento in ambienti diversi degli utenti o dei tecnici; riavvio su elaboratori di un sito secondario. In tali casi è possibile che sia necessario ricopiare o ricostruire i dati precedentemente disponibili ed effettuare controlli di corretto allineamento e di quadratura a cura dei tecnici o degli utenti. È molto importante il colloquio fra utenti e tecnici nella fase di gestione dell'emergenza; i tempi necessari per il ripristino dell'applicazione debbono essere costantemente monitorati in modo da consentire agli utenti di decidere se passare a soluzioni di *contingency*.

Nel caso di disastro, sapendo di non essere in grado di ripristinare la funzionalità dell'applicazione in tempo utile, occorre attivare procedure di *contingency* a cura degli utenti. Queste potrebbero sostituire in parte o del tutto l'applicazione in esame ed essere a loro volta di tipo automatico oppure manuale, con eventuale trasmissione di informazioni per fax o telefono. Il rientro dalla situazione di emergenza a quella di normale funzionamento richiede normalmente l'inserimento di dati trattati durante la fase di emergenza in modo manuale e opportuni controlli di corretto allineamento e di quadratura. Vale per le soluzioni di *contingency* quanto detto in tema di *checklist* per le altre tipologie di soluzione; anzi, in questo caso, la necessità di verifica e di certificazione è ancora più elevata, in quanto non esiste la *contingency* della *contingency*.

3.2.1.3 Struttura organizzativa preposta alla gestione dell'emergenza

Una volta individuati gli scenari di emergenza e le possibili soluzioni, occorre definire la struttura organizzativa preposta alla gestione dell'emergenza. Tale struttura, oltre ad attivarsi a fronte delle situazioni di emergenza e a porre in atto le misure necessarie a superarle, dovrebbe preoccuparsi: a) del monitoraggio della situazione di emergenza, fino al ripristino delle condizioni di normale operatività; b) del coordinamento dei *team* coinvolti; c) delle modalità di comunicazione interaziendale e con l'esterno; d) della gestione dell'*incident reporting*.

Occorre quindi definire un'altra struttura che si occupi di tali problematiche; essa deve operare in parallelo ai team di tecnici e utenti responsabili della soluzione del problema e potrà anche parzialmente sovrapporsi ad essi. A seconda della struttura e della dimensione dell'azienda, si potrà far ricorso all'*help desk* utilizzato per tutte le strutture informatiche.

Sarebbe anche opportuno definire: i) un *crisis manager*, se possibile espressione degli utenti dell'applicazione, responsabile delle comunicazioni con l'esterno e con la Direzione e dell'eventuale adozione di soluzioni di *contingency*; ii) un coordinatore tecnico, responsabile delle comunicazioni interaziendali e delle soluzioni tecniche e dell'eventuale *escalation* fra esse, fino al *disaster recovery* in un sito secondario, se previsto. Qualora più applicazioni vitali fossero interessate a una stessa situazione di emergenza, dovrebbero essere predefinite le priorità di intervento, a maggior ragione se fossero coinvolti coordinatori diversi.

Nella struttura preposta alla gestione dell'emergenza bisogna anche tenere conto del ruolo dei fornitori. Occorrerebbe fare in modo che i contratti di manutenzione delle infrastrutture e di assistenza sistemistica e applicativa prevedano tempi e modalità di intervento compatibili con le soluzioni individuate. Questo è tanto più vero quanto più si va verso forme di *outsourcing* esteso (ad esempio per l'intero centro elaborazione dati secondario da utilizzare in caso di *disaster recovery*), in cui si dovrebbe verificare periodicamente lo stato di adeguamento dei piani di emergenza dei fornitori a quelli aziendali. In caso di *outsourcing* esteso o in presenza di sistemi e reti esterni indispensabili alla funzionalità dell'applicazione, sarebbe quindi necessario stipulare con i fornitori specifici accordi sui livelli di servizio ed, eventualmente, ricorrere a opportune forme assicurative.

Per individuare le situazioni di emergenza, ogni azienda dovrebbe fare ricorso a strumenti automatici di controllo operativo, se possibile comuni a tutti i componenti del sistema informatico e logistico, quali quelli descritti nel par. 2.2.3. Questi strumenti consentono di ridurre i tempi di reazione e all'occorrenza di attivare, al di fuori dell'orario di lavoro, personale in reperibilità.

Per quanto riguarda il monitoraggio e l'*incident reporting*, ogni azienda dovrebbe dotarsi di procedure standardizzate di raccolta e presentazione delle informazioni relative alle diverse situazioni di emergenza occorse. Tali informazioni potrebbero essere utili a fini di *audit* e per costruire statistiche sulle quali sviluppare casi di studio per successive azioni correttive tecniche o organizzative. Soluzione ottimale sarebbe quella di disporre di una procedura automatica (e-mail, intranet, ecc.) integrata con un *data base*.

3.2.2 Gestione del BCP

Un BCP ben progettato è condizione necessaria ma non sufficiente per affrontare al meglio le situazioni di emergenza. Occorre infatti preparare il personale coinvolto, dirigenti, tecnici e utenti delle applicazioni critiche, alla gestione dell'emergenza. In presenza di situazioni critiche sono infatti cruciali le capacità di ripristinare l'operatività nel più breve tempo possibile e di individuare e attuare, se necessario, le idonee procedure di recovery o di emergenza previste dal BCP medesimo.

Una preparazione puntuale prevede:

- individuazione e disponibilità dello staff critico;
- addestramento del personale e test periodici;
- adeguamento periodico del piano.

Alla descrizione di come prepararsi all'emergenza segue quella delle procedure operative e delle regole di comportamento da adottare nel caso che l'emergenza si verifichi.

3.2.2.1 Individuazione e disponibilità dello staff critico

Parte rilevante del BCP è l'individuazione dello staff critico, composto da personale tecnico e utente che, all'interno della struttura organizzativa preposta alla gestione dell'emergenza, è in grado di intervenire durante il normale orario di lavoro e al di fuori di esso. Occorre assicurare, infatti, la disponibilità di tutte le figure professionali, nella misura minima necessaria e in tempi compatibili con quelli previsti dagli scenari di emergenza e dalle possibili soluzioni. Potrebbe anche essere necessario intervenire sull'organizzazione degli orari di lavoro, introducendo differenziazioni in entrata e in uscita e istituendo turni. Va ricordato che mentre ciò accade normalmente nella conduzione di un CED, per gli utenti di una applicazione è inusuale e di difficile adozione.

Sarebbe opportuno definire su base periodica un piano con l'elenco del personale incaricato, comprensivo di quello di fornitori esterni, e il relativo orario di presenza e di reperibilità. Il piano dovrebbe anche contenere le indicazioni per contattare i componenti dello staff critico (ad esempio numeri di cellulare, teledrin, ecc.) e renderli operativi nel più breve tempo possibile.

Il piano delle presenze e delle reperibilità dovrebbe essere reso disponibile con sufficiente anticipo a tutto il personale della struttura organizzativa interessata. Giorno per giorno dovrebbe poi esserne verificata la congruità, che potrebbe essere compromessa da assenze improvvise (ad esempio per malattia, sciopero, ecc.), procedendo se del caso a un aggiornamento e a una nuova distribuzione.

Particolare attenzione andrebbe posta anche alla definizione delle modalità di chiamata e di intervento dei fornitori per la riparazione di guasti e per la riattivazione di sistemi e reti esterni indispensabili alla funzionalità dell'applicazione vitale, se presenti. L'aver stipulato un buon contratto o un buon accordo sui livelli di servizio può, infatti, risultare non sufficiente se non viene posta adeguata attenzione a questi dettagli gestionali.

3.2.2.2 Addestramento del personale e test periodici

Lo staff critico, oltre a essere ben individuato quotidianamente dal piano delle presenze e delle reperibilità, deve essere sottoposto a idonee forme di preparazione, per far sì che il BCP possa essere attivato efficacemente.

Lo staff critico deve padroneggiare tutti gli argomenti trattati nello sviluppo del BCP e, in particolare, gli scenari di emergenza e le possibili soluzioni; ciascun componente dello staff critico deve conoscere il suo ruolo e le sue responsabilità, nonché l'importanza di seguire scrupolosamente le istruzioni del BCP. La preparazione deve comprendere anche esercitazioni e test, da condurre periodicamente.

Le esercitazioni e i test possono coprire per dato scenario di emergenza una o diverse soluzioni, oppure fermarsi a esaminare una specifica parte di una data soluzione, a seconda del livello di approfondimento richiesto. Un limite è posto dal costo dell'attività di addestramento, che cresce velocemente con il numero degli incontri addestrativi e del personale coinvolto, sia tecnico sia utente. I test richiedono, inoltre, quasi sempre, l'allestimento di specifici ambienti separati da quello di produzione, i cui costi possono essere assai elevati.

La predisposizione di una buona documentazione è essenziale, sia a fini didattici, sia per la gestione delle situazioni di emergenza. Caratteristiche essenziali per una consultazione rapida quale può essere quella in fase di emergenza sono il livello di aggiornamento e la sinteticità. Le esercitazioni e i test periodici possono essere utili per migliorare la documentazione disponibile. Esistono sul mercato prodotti atti a semplificare la produzione, l'aggiornamento e il reperimento della documentazione.

I test periodici, oltre ad avere fini addestrativi, consentono di verificare l'adeguatezza delle soluzioni e delle relative *checklist* predisposte per i vari scenari di emergenza, comprese quelle di *contingency*. Occorre distinguere fra test di tipo tecnico e test di *business*. I primi, relativi alle sole infrastrutture, coinvolgono solo i *team* tecnici, i secondi, che comprendono anche l'applicazione vitale nel suo funzionamento, anche i *team* utente. I test tecnici sono da considerare propedeutici a quelli di *business* e normalmente non consentono di verificare appieno la bontà del BCP. Un esempio tipico è quello del *disaster recovery*: la sua valenza è diversa a seconda che sia eseguito in condizioni di operatività, o meno, dell'applicazione. Il test è ancora più significativo, e consentirebbe di verificare non solo la bontà teorica del BCP, ma anche quella pratica, se effettuato senza preavviso. Non è però detto che sia facile o possibile eseguire un test di *business* programmato con preavviso o senza.

Occorre quindi progettare ed eseguire test che soddisfino requisiti minimi tali da consentire di certificare la bontà del BCP. Tali test dovrebbero essere validati da *auditor* interni o esterni ed eseguiti con periodicità prefissata. Anche i risultati dovrebbero essere controllati e validati. Specifica documentazione dovrebbe essere prodotta, comprensiva di anomalie e problemi riscontrati e dell'indicazione di coloro che dovranno analizzarli e risolverli.

3.2.2.3 Adeguamento periodico del piano

Un BCP è adeguato solo se è aggiornato. Variazioni si possono rendere necessarie a seguito di: a) modifiche alle componenti del sistema informatico e logistico utilizzato dall'applicazione vitale; b) modifiche all'applicazione vitale; c) modifica alle procedure di *contingency*; d) modifiche di tipo organizzativo e del business aziendale.

Occorre quindi individuare per il BCP precise modalità di manutenzione correttiva ed evolutiva e le figure coinvolte. Il processo da eseguire è ciclico: ogni volta occorre rivedere gli scenari di emergenza, le possibili soluzioni, la struttura organizzativa preposta alla gestione dell'emergenza, l'individuazione e disponibilità dello staff critico, l'addestramento del personale e i test periodici.

Particolare attenzione dovrebbe quindi essere data alla revisione e distribuzione della documentazione e al controllo dell'intero processo. Infine, il BCP potrebbe essere periodicamente certificato da *auditor* interni o esterni.

3.2.2.4 Gestione delle situazioni di emergenza

È essenziale disporre di un BCP aggiornato e di personale ben individuato e addestrato per gestire al meglio una situazione di emergenza, in cui è cruciale ripristinare l'operatività nel più breve tempo possibile. Occorre infatti tenere presente che una situazione di emergenza effettiva difficilmente coincide con una simulata e che lo stress a cui è soggetto il personale coinvolto è assai più elevato. Inoltre, i test periodici dei piani di emergenza sono usualmente eseguiti da *team* completi, mentre in una situazione effettiva alcuni componenti dello staff critico potrebbero non essere presenti e neppure reperibili. Ciò è sicuramente vero se l'emergenza si presenta fuori dal normale orario di lavoro, quando il presidio di personale tecnico è ridotto o mancante del tutto.

L'utilizzo di strumenti automatici di controllo operativo che possano inviare allarmi a personale in reperibilità e la possibilità per il personale tecnico di intervenire remotamente sulle componenti più critiche del sistema informatico dovrebbe essere preso in considerazione nel caso di applicazioni vitali per l'azienda.

In presenza di una situazione di emergenza, tutto il personale coinvolto è tenuto a rispettare le regole previste nel BCP e in particolare la suddivisione dei ruoli: è, ad esempio, essenziale che i tecnici impegnati nella soluzione del problema non siano distolti dall'attività da richieste di informazioni sull'incidente in corso. Il monitoraggio della situazione di emergenza e la comunicazione interaziendale e con l'esterno dovrebbero seguire i canali prestabiliti. L'*escalation* fra le diverse soluzioni tecniche e di *contingency*, governata dal responsabile tecnico e dal *crisis manager*, dovrebbe avvenire in base ai tempi e alle modalità stabilite in sede di definizione degli scenari di emergenza e delle relative soluzioni.

È possibile, comunque, che all'atto dell'emergenza una o più soluzioni previste non sia applicabile per il sopravvenire di problemi non previsti o non prevedibili (ad esempio un errore operativo, la mancanza di opportuni profili abilitativi, l'assenza di uno o più addetti dello staff critico, il presentarsi di un ulteriore evento critico, ecc.). Anche in questi casi, ove possibile, l'*escalation* dovrebbe essere quella prevista dal BCP. In ogni caso, il filo conduttore di tutta la gestione della situazione di emergenza dovrebbe essere sempre quello di minimizzare i rischi connessi con l'operatività e di massimizzare il livello di servizio agli utenti dell'applicazione vitale.

Una volta ritornati alla situazione di normale funzionamento del sistema informatico, occorre: a) ripristinare l'operatività dell'applicazione, eventualmente ricostruendo dati persi o trattati manualmente nella fase di emergenza, ed effettuare tutti i necessari controlli di corretto allineamento e quadratura; b) verificare che l'intervento sia stato eseguito a regola d'arte e non abbia creato i presupposti per una nuova situazione di emergenza; c) verificare ed eventualmente completare la documentazione richiesta per l'*incident reporting.*

4. CASE STUDY

4.1 DESCRIZIONE DELL'APPLICAZIONE E DEI REQUISITI DI CONTINUITÀ DI SERVIZIO

L'applicazione da sviluppare presa in esame riguarda i "Sistemi di Pagamento" e più in particolare: i bonifici, i girofondi estero con controparte bancaria italiana, i pagamenti con controparte estera.

I Settori dell'Azienda, direttamente o indirettamente, interessati sono: Tesoreria, Estero – Ufficio Accentratore, Incassi e Pagamenti, Filiali Italia, Organizzazione e Sistemi Informativi.

I collegamenti interessati sono quelli tra il CED e la Tesoreria, Estero – Ufficio Accentratore, le Filiali Italia, la Banca d'Italia.

I Settori dell'Azienda direttamente o indirettamente interessati all'applicazione hanno fissato i seguenti requisiti di continuità di servizio:

- ⇒ la fascia oraria giornaliera di operatività è quella del normale orario di lavoro bancario;
- ⇒ eventuali interruzioni di servizio in tale fascia oraria non possono superare complessivamente il limite di due ore al giorno, per non più di una volta al mese;
- ⇒ devono essere rispettati i tempi di *cut off* previsti dalle procedure BI-REL (sistema nazionale di regolamento lordo), TARGET (sistema europeo di regolamento lordo) ed EBA *clearing* (sistema di compensazione per i pagamenti al dettaglio in Euro);
- ⇒ deve essere assicurata in ogni caso la lavorazione dei bonifici di importo maggiore o uguale a Lit. 500 milioni.

Nell'ambito dell'analisi dei rischi è stato valutato che il livello di rischio associato al non rispetto di tali requisiti è così alto per l'Azienda da dover annoverare l'applicazione in esame tra quelle "vitali". Verranno quindi seguite nelle fasi progettuali e nella gestione corrente la metodologia di analisi e le regole di comportamento illustrate nel documento CIPA "Continuità di servizio e gestione dell'emergenza" e, in particolare, sarà approntato un *Business Contingency Plan* già durante le fasi progettuali.

4.2 SISTEMA INFORMATICO E LOGISTICO

L'applicazione in esame dovrebbe operare sul sistema informatico e logistico già presente in Azienda. Occorre quindi innanzitutto verificare se esso è idoneo a garantire gli stringenti requisiti di continuità di servizio richiesti.

Le principali caratteristiche informatiche e impiantistiche dei centri elaborazione dati sono le seguenti:

- **CED**

  - **Impianto di alimentazione elettrica.**
    Ente erogatore: accordi prevedono la fornitura del servizio con collegamento diretto alla rete in media tensione attraverso due distinte consegne.
    Batterie tampone: sono sufficienti a garantire il corretto funzionamento delle apparecchiature, elettroniche e non, installate nel CED per il tempo necessario all'accensione dei generatori autonomi e, in ultima ipotesi, ad una chiusura ordinata delle applicazioni.
    Generatori autonomi: 3 sistemi a turbina erogano l'alimentazione necessaria al funzionamento delle apparecchiature elettroniche e dei principali servizi ausiliari. La loro potenza è stata calcolata in modo che 2 di essi sono sufficienti alle necessità del caso.
    Quadri elettrici: le utenze HW prevedono la doppia alimentazione da quadri distinti.

  - **Impianto di condizionamento.**
    Le apparecchiature installate sono ridondanti e assicurano le normali condizioni di funzionamento degli elaboratori; il loro numero è tale da garantire il condizionamento dei sistemi a fronte di guasti e manutenzioni.

  - **Elaboratori.**
    I 3 *mainframe* del CED di produzione sono dimensionati in modo che l'eventuale malfunzionamento di uno di essi non crei apprezzabili disservizi.
    Gli elaboratori sono connessi in architettura SYSPLEX.
    Coupling facility: 2 in mutuo *recovery*.
    Dischi magnetici: le stringhe di dischi sono condivise tra le varie unità centrali di elaborazione; tutte le unità sono "RAID 5" e il loro numero è superiore alle effettive esigenze di memorizzazione.
    Canali: la ridondanza dei canali è completa, risultando più che duplicati (per la quasi totalità addirittura quadruplicati) gli accessi alle varie periferiche.
    Front end processor: i "FEP" (in totale 4 fisici, 2 logici) sono anch'essi ridondati a coppia.
    Datacenter CISCO : infrastruttura a più livelli di *router* per l'instradamento del traffico SNA verso i *mainframe*.
    Cartucce: le unità di lettura/registrazione sono servite da appositi "robot" (6 per l'ambiente di produzione) e sono accessibili da tutti i sistemi; la gestione è completamente automatizzata. In una nastroteca esterna ai locali del CED sono custodite le seconde copie (quelle di sicurezza) dei salvataggi del *software* (di base, gestionale e applicativo) e dei dati applicativi (*image copy* settimanali e *log* giornalieri).

  - **Software di Base.**
    Sulle 3 macchine di produzione è installato lo stesso *software* di base (MVS) e la quasi totalità delle applicazioni è in IMS.
    Inoltre, per garantire un corretto bilanciamento del carico e per facilitare la manutenzione dei sistemi sono attivi: il *full data sharing*, che consente lo *sharing* sia dei dati DL/I che di quelli DB2; la funzione *workload balancing* dell'IMS, che consente la schedulazione delle transazioni su una qualunque delle macchine di produzione,

collegate in *parallel sysplex*; la funzione "VGR" (*Vtam Generic Resource*), che di fatto consente al VTAM di vedere i vari sottosistemi IMS come un tutt'uno.

- **CENTRO DI DISASTER RECOVERY**

  Presso il centro di *disaster recovery* sono installate la capacità elaborativa e le apparecchiature necessarie per il ripristino dell'operatività. Il piano di *disaster recovery* prevede il ripristino presso il CED secondario, entro l'inizio della successiva giornata lavorativa, di tutte le applicazioni in produzione, utilizzando le copie di salvataggio in nastroteca di sicurezza, esterna al CED. In particolare la ricostruzione dei dati applicativi fino all'ultimo aggiornamento effettuato prima del fermo consiste nei seguenti passi: a) caricamento dell'*image copy* della settimana precedente*;* b) ricostruzione dei dati della settimana corrente a partire dai *log* giornalieri; c) inserimento manuale dei dati relativi alla giornata in cui è avvenuto il fermo.

- **FILIALE**

  - **Alimentazione elettrica.**
    Presso ogni filiale sono installate batterie tampone sufficienti ad assicurare la chiusura ordinata delle applicazioni, ma non la continuità di funzionamento delle apparecchiature. Per alcune sedi l'alimentazione è assicurata da due cabine diverse dell'ente erogatore.

  - **Server NT.**
    CPU: 2 CPU, contemporaneamente funzionanti, l'una in grado a sopperire ad un eventuale malfunzionamento dell'altra (il *back-up* non è a caldo, essendo previsto il *restart* della macchina funzionante).
    Schede di rete: 2 schede ETHERNET, entrambe attive.
    Dischi: dischi RAID 5 (in caso di rottura di un disco, gli altri continuano a funzionare e il *recovery* del disco guasto viene effettuato automaticamente su un altro disco.

  - **Client NT.**
    Non ha niente di duplicato. In caso di un qualunque malfunzionamento, è previsto il fermo del posto di lavoro.

  - **Rete locale.**
    Router: non duplicato.
    Switch: utilizzato come concentratore dei segmenti di LAN; non duplicato.

  - **Rete Geografica.**
    La rete è ISDN (di tipo *frame relay business frame*), già ridondata al suo interno. Se la "coda urbana" che collega alla centrale telefonica si interrompe, il collegamento è comunque garantito in automatico (*backup on demand*).

L’infrastruttura informatica del CED presenta caratteristiche di ridondanza idonee a garantire, in assenza di eventi eccezionali, i livelli di servizio richiesti per l’applicazione vitale in esame. In caso di *disaster recovery*, la soluzione esistente che richiede tempi di ripristino dell’ordine di una giornata non consente di rispettare i requisiti di continuità di servizio richiesti.

Nel caso delle filiali, le infrastrutture informatiche non sono sufficientemente ridondate a impedire il fermo dell’operatività a fronte di guasti alla rete locale o a mancanza di alimentazione elettrica. È però sempre possibile riprendere l’operatività presso i locali e i terminali di una filiale limitrofa nel tempo massimo previsto di due ore.

Tenendo conto di questo quadro, il Capo Progetto decide che non valga la pena effettuare nuovi investimenti informatici per ridurre i “rischi residui”; tuttavia decide, insieme agli utenti, di adottare soluzioni di *contingency* manuali per fronteggiare gli eventuali malfunzionamenti che possano pregiudicare il livello di continuità di servizio richiesto. Queste soluzioni fanno parte integrante del BCP.

4.3 SVILUPPO DELL’APPLICAZIONE E ASPETTI DI SICUREZZA

Per quanto riguarda il *software* applicativo, la componente centrale è sviluppata in COBOL e opera in MVS, sottosistema IMS e quella locale è sviluppata in “*Visual Age*” e *“Small Talk”*, con ambiente operativo WINDOWS NT.

L’applicazione viene realizzata con una certa modularità per facilitare al massimo le eventuali attività di aggiornamento e gli agganci con altre applicazioni. Prevede, inoltre, controlli di quadratura che risultano adeguati alla delicatezza dei dati trattati. L’applicazione, pur essendo correlata ad altre, prevede anche tecniche di colloquio asincrono che la rendono in qualche modo indipendente dalle stesse. Le normali operazioni di gestione (batch serale, salvataggi, ecc.) non influenzano la normale operatività. È stata posta particolare attenzione alla progettazione ed esecuzione dei test, mentre non si è ritenuto necessario ricorrere al controllo di qualità.

La documentazione, redatta secondo gli standard aziendali, facilita la tempestività degli interventi dei programmatori e degli addetti all’*help desk* e ai sistemi centrali (presidi operativi) a fronte di anomalie di funzionamento.

Non sono previste modifiche all’attuale sistema SW di controllo degli accessi, già presente sugli elaboratori centrali (RACF) e sulle piattaforme locali (*security* NT).

Tutti gli accessi, sia di sola lettura sia di aggiornamento ai dati, sono registrati sui giornali di sistema**;** le operazioni contabili vengono registrate anche su un apposito archivio applicativo (giornale di fondo, disponibile anche localmente).

Periodicamente vengono effettuate le copie di sicurezza dei dati, che vengono custodite presso la nastroteca esterna. I dati trasmessi in rete sono crittografati e autenticati.

4.4 BUSINESS CONTINGENCY PLAN

4.4.1 Scenari di emergenza e soluzioni

Di concerto con i Settori dell'Azienda interessati, sono stati individuati i vari scenari di emergenza e ipotizzate le possibili soluzioni.

Nella tabella che segue viene rappresentata una possibile schematizzazione dei principali scenari di emergenza in cui nelle righe sono indicate tutte le componenti interessate; nella prima colonna è riportato il tempo massimo di fermo prima del passaggio automatico a soluzioni di "*contingency* estrema" a cura degli utenti e nelle altre colonne sono indicati i possibili eventi, per semplicità qui accorpati in cinque diverse tipologie.

Ogni incrocio rappresenta una possibile situazione di emergenza. I valori riportati indicano la relativa gravità: 1-incidente; 2-incidente grave; 3-situazione di crisi; 4-disastro.

Componenti interessate	ore max fermo	Mancanza alimentazione elettrica da ente erogatore	Guasti agli impianti e ai sistemi	Malfunzione SW	Mancanza collegamenti rete esterna	inagibilità locali
intero CED	2					3-4
Impianto di condizionamento	24		1-4			
1 elaboratore su 3	---		1	1	1	
2 elaboratori su 3	3		3-4	3-4	3-4	
3 elaboratori su 3	2		3-4	3-4	3-4	
1 coupling facility	---		1			
2 coupling facility	---		1			
dischi e canali	---		1			
1 fep	---		1	1	1	
2 fep	2		3-4	3-4	3-4	
1 datacenter cisco	---		1	1	1	
2 datacenter cisco	2		3-4	3-4	3-4	
SW di base gestionale	---			1-2		
SW applicativo centrale	2			3-4		
Locali filiale	4	3-4				3-4
SW applicativo periferico	24			3-4		
1 server di filiale	---	1	1	1		
2 server di filiale	24	3-4	3-4	3-4		
Componenti di rete di filiale	24	3-4	3-4		3-4	

I tecnici debbono adoperarsi per risolvere la situazione di emergenza entro il tempo massimo indicato nella prima colonna; qualora ciò non sia possibile si prefigurerà una situazione di disastro.

Per ognuna delle situazioni di emergenza individuata, dovrebbero essere descritte le possibili soluzioni. Tuttavia, per brevità, non vengono trattate le situazioni risolvibili con il solo intervento dei tecnici (incidenti, incidenti gravi e situazioni di crisi). Ci si limiterà qui a descrivere una possibile soluzione da adottare per gli scenari di disastro relativi al CED. In questi casi, essa prevede come azione una operatività "degradata", a cura della Tesoreria, ricorrendo alla spedizione di supporti cartacei per fax o tramite corriere per adempiere le disposizioni ricevute dalle controparti bancarie o dalla clientela. In particolare:

- il coordinatore tecnico fornisce al *crisis manager* una stima del livello di gravità della situazione e il *crisis manager* decide l'avvio della procedura di *contingency;*
- l'*help desk***,** mediante messaggio in posta elettronica o con un mezzo alternativo, avvisa le Filiali della situazione di "emergenza" e della prevista durata della stessa;
- la Tesoreria informa il sistema interbancario, tramite messaggio libero MID (Mercato Interbancario Depositi, attestato su un *server* dedicato della SIA) o fax, che la situazione di "emergenza" implica il ricorso a pagamenti cartacei per la prevista durata del disservizio;
- la generica Filiale:
  - invia all'Ufficio Accentratore – Estero le disposizioni di pagamento dei clienti;
  - contestualmente, preavvisa la Tesoreria dell'ammontare dei pagamenti stessi;
  - registra le operazioni con una procedura *off-line* o, nel caso in cui questa non funzioni, sulle schede clienti;
- l'ufficio Accentratore – Estero invia le istruzioni disposte manualmente alla Banca d'Italia, attraverso la spedizione degli ordini di addebito e accredito in giornata su supporto cartaceo (entro le ore 17:00 per le transazioni commerciali e le 18:00 per quelle interbancarie);
- lo stesso ufficio invia alla Banca d'Italia le istruzioni cartacee relative ai girofondi estero con controparte bancaria italiana;
- una risorsa dell'area Estero in stretto contatto con la Banca d'Italia fornisce alla Tesoreria ogni dettaglio in merito ai pagamenti in arrivo e all'aggiornamento del saldo del conto di gestione.

Una volta superata l'emergenza:

- il coordinatore tecnico notifica il ripristino al *crisis manager* e l'*help desk* alle strutture di base interessate, ad eccezione delle filiali;
- il centro servizi riceve le contabili emesse manualmente ed effettua l'inserimento dei dati relativi in procedura, controllandone l'allineamento e la quadratura;
- la Tesoreria, accertato il normale deflusso e il regolamento delle disposizioni, invia comunicazione di cessata emergenza a tutto il sistema mediante messaggio libero;
- l'*help desk* informa le filiali del superamento della situazione di emergenza.

Nel caso in cui i tempi di ripristino fossero superiori alla giornata e per i soli problemi infrastrutturali, in parallelo, si darà avvio alla procedura di *disaster recovery* per consentire l'apertura della nuova giornata operativa sugli elaboratori del *sito di disaster recovery.* Tale procedura può essere attuata solo dopo la dichiarazione dello stato di emergenza da parte del Comitato per la Sicurezza Aziendale.

4.4.2 Struttura organizzativa per la gestione dell'emergenza

Particolare attenzione è stata posta ai *team* coinvolti, alle strategie di coordinamento e alle modalità di comunicazioni interaziendali e con l'esterno.

Presso la Tesoreria viene costituita la seguente struttura organizzativa preposta alla gestione dell'emergenza:

Crisis Manager	risorsa della Tesoreria, responsabile delle comunicazioni con l'esterno e con la Direzione, delle soluzioni di *contingency* e della loro attivazione; Sig. …….. Tel. Cell. ……. Sostituto Sig. ……. Tel. Cell. ……
Coordinatore Tecnico	risorsa dell'area Organizzazione e Sistemi Informativi, responsabile delle comunicazioni interaziendali, delle soluzioni tecniche e dell'*escalation* fra esse; coordina gli interventi dei tecnici di fornitori esterni e cura il monitoraggio e la stesura dell'*incident reporting*; Sig. …….. Tel. Cell. ……. Sostituto Sig. ……. Tel. Cell. ……
Specialisti amministrativi	risorse al momento disponibili tra il personale di Tesoreria, specializzate nella materia, per fornire assistenza agli utenti; VEDI LISTA REPERIBILITA' DEL MESE per interventi al di fuori dell'orario di lavoro.
Specialisti tecnici	risorse dell'area Organizzazione e Sistemi Informativi, prese tra quelle al momento disponibili, di supporto tecnico;

VEDI LISTA REPERIBILITA’ DEL MESE per interventi al di fuori dell’orario di lavoro.

4.4.3 Addestramento del personale e test periodici

Per gli appartenenti alla struttura di gestione dell’emergenza, nella settimana precedente l’avvio in produzione e a seguire periodicamente, con cadenza semestrale, è previsto un test delle principali procedure di *recovery* e di *contingency*. Detto test è finalizzato alla formazione del personale, e alla verifica della documentazione, che è disponibile presso le segreterie delle strutture interessate e presso la nastroteca di sicurezza.

5. APPENDICE

5.1 DEFINIZIONE DI APPLICAZIONE VITALE

Un'applicazione è "vitale" quando il livello di rischio di conseguenze particolarmente negative associato a una sua indisponibilità è "alto".

Una valutazione del rischio legato all'indisponibilità dovrebbe essere effettuata prima dello sviluppo dell'applicazione stessa, sotto la supervisione del responsabile del progetto, e tener conto:

a) del processo in termini di flussi operativi e della relativa integrazione nel quadro aziendale;

b) della possibilità di eseguire il processo, del tutto o in parte, anche in caso di malfunzionamento o indisponibilità dell'applicazione.

Parametri guida per la valutazione del rischio sono:

- l'importanza del processo nel business aziendale;
- i vincoli di sistema o legislativi da rispettare;
- il tempo accettabile di fermo;
- il grado di avversione al rischio dell'azienda.

In ambito bancario, ad esempio, va garantita:

- la funzionalità di un servizio minimale alla propria clientela, per consentire almeno le operazioni essenziali (es. prelievo e deposito contante, operatività sul mercato finanziario);
- la funzionalità delle infrastrutture di comunicazione con il sistema bancario nazionale e internazionale (rete interbancaria, SWIFT, ecc.).

Una volta sviluppato il progetto relativo a una data applicazione "vitale", che comprende la definizione delle infrastrutture di sistema e di rete, del *software* di base e applicativo e delle basi informative, il rischio residuo, dovuto ai livelli di minaccia e di vulnerabilità a cui tali *asset* sono soggetti, dovrà essere illustrato e sottoposto all'approvazione della Direzione, cui spetta la decisione finale.

5.2 ANALISI DEL RISCHIO

L’analisi del rischio consiste nell’individuazione dei possibili eventi che potrebbero provocare danni nello svolgimento di un processo aziendale che si intende automatizzare ricorrendo a una applicazione informatica. Tali eventi si configurano come rischi quando la probabilità di accadere non è trascurabile.

L’analisi del rischio deve essere condotta dalle fasi iniziali della progettazione e si sviluppa nei seguenti passi:

1) acquisizione da parte del gruppo di progetto dei requisiti di sicurezza richiesti dall’utente dell’applicazione;

2) identificazione da parte del gruppo di progetto degli elementi del sistema informatico e logistico in cui collocare l’applicazione in oggetto;

3) analisi degli eventi che possono danneggiare il funzionamento dell’applicazione;

4) valutazione delle misure esistenti per la protezione da tali eventi; se queste non soddisfano i requisiti di sicurezza previsti, va condotta un’analisi aggiuntiva per quantificare la dimensione del rischio residuo.

Se il rischio residuo non è considerato accettabile, sarà necessario individuare idonei interventi di adeguamento del sistema informatico e/o logistico che dovranno essere approvati dalla Direzione, assieme con l’accettazione di quella componente di rischio che comunque non potrà essere eliminata.

L’analisi deve essere effettuata con riferimento a tutti i possibili rischi (disponibilità, riservatezza, integrità, autenticazione, controllabilità, non ripudio).

In particolare in questo lavoro si è prevalentemente interessati alla disponibilità.

Fra gli aspetti che consentono di individuare i requisiti di disponibilità si ricordano i seguenti:

- fascia oraria giornaliera di operatività dell’applicazione in condizioni normali;
- tempi di risposta richiesti per le varie operazioni;
- eventuali tempi di *cut off*;
- tempi da rispettare o limite per la disponibilità dei risultati;
- adempimenti legali e contrattuali;
- vincoli finanziari;
- criticità del sistema ed eventuali implicazioni del *disaster recovery*.

Le domande cui è necessario rispondere per individuare gli eventuali interventi sul sistema logistico e informatico sono:

- Quali sarebbero le conseguenze se l’applicazione fosse solo parzialmente operativa?
- Quali se un guasto o un disastro la rendessero totalmente non operativa?

Al riguardo, dovrebbero essere prese in considerazione:

- *le conseguenze di non avere accesso ai dati (aggiornati);*
- *le conseguenze di non avere accesso al sistema;*
- *le conseguenze per altre applicazioni dipendenti da quella in oggetto.*

- Qual è il limite di tempo di indisponibilità dell'applicazione perché si comincino ad avvertire le prime conseguenze?
- Dopo quante ore/giorni l'indisponibilità dell'applicazione diventa inaccettabile?
- Ci sono modalità alternative per trattare le informazioni e mandare avanti il *core business*, anche se su base temporanea, e per quanto tempo possono essere utilizzate?
- Sulla base dell'esperienza acquisita quali sono i potenziali punti deboli del sistema e da chi o da che cosa sarebbero originati?

6. GLOSSARIO

Il presente glossario ha lo scopo di agevolare la comprensione dei termini più strettamente tecnici presenti nel documento. Al fine di rendere più agevole la consultazione, sono stati esclusi dal glossario i termini il cui uso è ormai entrato a far parte del linguaggio comune, quali ad esempio *software, hardware, personal computer,* ecc.

Per ogni voce è stata fornita una descrizione sintetica, con particolare riferimento alla specifica valenza attribuita nel testo. Talune definizioni possono presentare pertanto differenze rispetto a quelle cui fa normalmente riferimento la letteratura in materia.

AFFIDABILITÀ
Capacita di un sistema di fornire i risultati attesi.

ANALISI DEI RISCHI (RISK ANALYSIS)
Valutazione (qualitativa e/o quantitativa) delle possibili MINACCE (V.) e delle probabilità con cui esse possono provocare danni al sistema (una *minaccia* diventa un RISCHIO (V.) quando la probabilità non è trascurabile e l'impatto sul sistema è significativo);

ANTIVIRUS
Componente software (o hardware) in grado di verificare l'eventuale presenza di un VIRUS INFORMATICO (V.) su di un supporto magnetico o un sistema elaborativo, di identificarlo e distruggerlo e, se possibile, di ripristinare lo stato normale di funzionamento. Alcuni *antivirus* svolgono anche la funzione di scudo protettivo contro le possibili infezioni da virus noti.

APPLICAZIONI CLIENT/SERVER
Particolare tipo di APPLICAZIONE DISTRIBUITA (V.) in cui parte di essa, residente su un CLIENT (V.) chiede e ottiene dei servizi elaborativi o dei dati da un altro sistema utilizzato come SERVER (V.).

APPLICAZIONI DISTRIBUITE
Applicazioni in cui la funzione elaborativa e/o i dati sono distribuiti su più sistemi, anche di tecnologia diversa (PC, SISTEMI INTERMEDI (V.), SISTEMI CENTRALI (V.)) che *cooperano* tra loro.

APPLICAZIONE VITALE
Applicazione in cui il livello di RISCHIO (V.) associato alla sua *indisponibilità* (V. DISPONIBILITÀ) è alto.

AUDIT (AUDITING)
Revisione o verifica delle procedure contabili, organizzative, informatiche e di controllo interno esistenti in azienda, avente lo scopo di determinare la conformità con criteri prestabiliti. L'*audit* può essere eseguito da revisori interni o esterni all'azienda.

AUDITABILITY
V. CONTROLLABILITÀ.

AUTENTICAZIONE
Determinazione inequivocabile dell'effettiva identità di una Entità (mittente o destinatario), soggetto di una trasmissione (*peer-entity authentication*) ovvero dell'effettiva origine dei dati trasmessi (*data-origin authentication*).

AUTORIZZAZIONE
Concessione (e successivo legittimo possesso) di diritti di accesso o di utilizzo di risorse o di oggetti.

BACKUP
MISURA DI RECOVERY (v.) finalizzata a costituire una disponibilità aggiuntiva di risorse, attraverso la duplicazione delle informazioni (*copie di backup*) o attraverso la disponibilità di risorse aziendali aggiuntive (infrastrutture, dispositivi hardware, personale, ecc.) .

BATCH
Ambiente o modalità elaborativa di massa, in cui i dati vengono elaborati senza interazione con l'utente. Si contrappone all'ambiente o alla modalità *transazionale*, in cui l'utente interagisce col sistema per effettuare singole *transazioni* e ottiene un riscontro immediato sull'esito delle transazioni stesse.

BUSINESS CONTINGENCY PLAN (BCP)
L'insieme delle possibili soluzioni, i team coinvolti, le strategie di coordinamento, le modalità di comunicazione interaziendali e con l'esterno, previsti per le varie tipologie di situazioni di emergenza relative a una APPLICAZIONE VITALE (V.). Comprende anche le MISURE DI CONTINGENCY (v.) da adottare nel caso non sia possibile garantire il ripristino della funzionalità dell'applicazione nei tempi massimi previsti.

BUSINESS CONTINUITY PLAN
L'insieme delle modalità e dei tempi di effettuazione relativi alle MISURE DI RECOVERY (v.) da adottare per superare una situazione di emergenza e ripristinare le funzionalità di un'applicazione all'interno del lasso massimo di tempo disponibile. Il *business continuity plan* può includere tra le misure previste anche il DISASTER RECOVERY (v.).

CANALI
Dispositivi hardware che gestiscono il trasferimento dei dati tra un elaboratore e i suoi dispositivi periferici o tra elaboratori.

CAPACITY PLANNING
L'insieme delle attività di misurazione delle prestazioni dei sistemi, di reporting e di valutazione, finalizzate a dimensionare i sistemi elaborativi in funzione della previsione di variazione nel tempo del carico elaborativo, attraverso l'utilizzo di modelli analitici o di simulazione.

CED
Centro elaborazione dati, generalmente dotato di uno o più SISTEMI CENTRALI (V.) e/o SISTEMI INTERMEDI (V.), di FRONT-END PROCESSOR (V.) per la gestione delle connessioni a reti trasmissione dati, di adeguate infrastrutture tecnologiche e di strutture di supporto, organizzativo e gestionale. Tale complesso di risorse può anche essere geograficamente distribuito sul territorio.

CHANGE MANAGEMENT
Insieme delle azioni riguardanti la proposta, la valutazione, l'approvazione e la gestione delle modifiche alle componenti software (applicativo e di base) e hardware del sistema informatico aziendale.

CLIENT
Sistema che viene utilizzato nell'ambito delle applicazioni CLIENT/SERVER (V.) per chiedere e ottenere servizi da altri sistemi che svolgono funzioni di SERVER (V.).

CLUSTER
Complesso di apparecchiature governate da un unico sistema di controllo/gestione.

CLUSTERING
Accoppiamento di due o più sistemi omogenei, finalizzato alla condivisione degli stessi dispositivi di memorizzazione.

CLUSTERING REMOTO
CLUSTERING (V.) tra sistemi collegati remotamente con fibre ottiche. I dati devono essere replicati presso i vari sistemi.

CONFIDENZIALITÀ
V. RISERVATEZZA

CONTINUITÀ DI SERVIZIO
Parametro da considerare in sede di progettazione di una applicazione, consistente nell'intervallo temporale in cui deve essere erogato il servizio, comprensivo del numero e dei tempi di fermo massimi accettabili. La *continuità di servizio* dovrebbe essere oggetto di contrattualizzazione nel caso di APPLICAZIONI VITALI (V.).

CONTROLLABILITÀ (AUDITABILITY)
Proprietà delle procedure applicative di rendere più facili e affidabili le verifiche, da parte delle funzioni di AUDIT (v.), della rispondenza alle specifiche e della correttezza della progettazione e dell'utilizzazione delle procedure stesse.
Tale proprietà va generalmente prevista e realizzata in sede di progetto/sviluppo delle applicazioni, ad esempio per mezzo di registrazioni degli eventi più significativi (V. TRACCE DI AUDIT).

COUPLING FACILITY
Dispositivo per la condivisione dei dati e il colloquio tra più sistemi in PARALLEL SYSPLEX (V.).

CPU (CENTRAL PROCESSING UNIT)
V. PROCESSORE.

CUT OFF
Orario limite entro il quale devono accadere determinati eventi (es. chiusura dei mercati telematici) od oltre il quale non sono più possibili o non sono più accettabili determinati eventi.

DISASTER RECOVERY
Insieme di procedure tecniche e organizzative attivate a fronte di un evento catastrofico che provochi l'indisponibilità completa del sito primario di elaborazione dati. L'obiettivo è riattivare le applicazioni vitali per l'azienda in un SITO DI DISASTER RECOVERY (v.). Vedi anche MISURE DI RECOVERY.

DISASTRO
Problema con impatti interni o esterni all'azienda che non è risolvibile nei tempi di ripristino previsti. In caso di *disastro* è necessario adottare le previste MISURE DI CONTINGENCY (v.).

DISPONIBILITÀ
Proprietà per cui le risorse sono accedibili e utilizzabili al momento della richiesta e con continuità da parte delle entità o dei soggetti autorizzati. Opposto: *Indisponibilità.*
Normalmente come misura della *disponibilità* si adotta il rapporto tra il tempo di servizio effettivamente erogato e il tempo di servizio previsto (CONTINUITÀ DI SERVIZIO (V.)). Si ha *alta disponibilità* quando tale rapporto si avvicina a uno.

E-MAIL
Modalità di scambio di messaggi, eventualmente corredati da allegati di vario tipo, via Internet o attraverso le reti Intranet aziendali.

EMPTY SHELL
V. SITO DI DISASTER RECOVERY

ESTERNALIZZAZIONE
V. OUTSOURCING

FAULT-TOLERANCE
Capacità, intrinseca e autonoma, di un'apparecchiatura (elettrica, elettronica, ecc.) di superare automaticamente eventuali guasti interni assicurando la continuità del servizio, eventualmente con prestazioni degradate.

FEP
V. FRONT END PROCESSOR.

FIREWALL
SISTEMA INTERMEDIO (V.) che si frappone tra la rete interna aziendale e le reti esterne (tipicamente *Internet*), al fine di impedire intrusioni da parte di terzi non autorizzati (es. *hackers*).

FIRMA DIGITALE
Tecnica utilizzata per consentire il NON RIPUDIO (v.) delle transazioni. E' basata sull'utilizzo di *chiavi asimmetriche* di cifratura, in cui il mittente "firma" la transazione attraverso una *chiave*

privata da lui solo posseduta; il destinatario può verificare l'autenticità della *firma digitale* per mezzo della *chiave pubblica* del mittente, rilasciata da una Autorità di Certificazione ufficialmente riconosciuta.

FRONT END PROCESSOR (FEP)
Apparato elettronico dedicato alla gestione delle connessioni a reti di trasmissione dati.

GEOGRAPHICALLY DISPERSED PARALLEL SYSPLEX
V. PARALLEL SYSPLEX

GESTIONE DEL RISCHIO (RISK MANAGEMENT)
Processo iterativo basato sull'ANALISI DEI RISCHI (v.), seguita da eventuali *interventi addizionali* per la riduzione dei RISCHI (V.) rilevati e dall'*accettazione* formale dei *rischi* residui.

HEARTBEAT
Segnalazioni prodotte a intervalli regolari (in analogia al battito del cuore) dai sistemi che devono essere tenuti sotto controllo, per poterne verificare il regolare funzionamento.

HELP DESK
Struttura di supporto di primo livello all'utenza interna e/o esterna per tutte le problematiche connesse alla fruizione dei servizi informatici dell'azienda.

HUB
Apparato di concentrazione e distribuzione del sistema di cablaggio della rete locale.

IMAGE COPY
Copia del contenuto di una base dati in cui oltre alle informazioni vengono mantenuti i legami logici e gli indici relativi alle stesse. Può essere utilizzata a fini di BACKUP (v.) o per riorganizzare la base dati stessa, al fine di migliorarne l'efficienza in termini di prestazioni e di spazio occupato.

INCIDENTE
Problema che non ha impatto nei confronti degli utenti interni ed esterni all'azienda, che viene risolto nei tempi massimi previsti, eventualmente applicando idonee MISURE DI RECOVERY (v.).

INCIDENTE GRAVE
Problema che ha impatto nei confronti di utenti interni all'azienda, che viene risolto nei tempi massimi previsti, eventualmente applicando idonee MISURE DI RECOVERY (v.).

INFORMAZIONI DI PARITÀ
V. RAID.

INTEGRITÀ
Integrità dei dati: proprietà delle informazioni di non essere alterate o distrutte in maniera non autorizzata.
Integrità dei sistemi: proprietà di un sistema di svolgere le funzioni previste, in assenza di manipolazioni non autorizzate deliberate o accidentali.

ISDN (INTEGRATED SERVICES DIGITAL NETWORK)
Tecnica standard per reti digitali, che consente di ottenere velocità di trasmissione e larghezza di banda maggiori rispetto alle tecniche tradizionali.

LIVELLI DI SERVIZIO
Requisiti di qualità del servizio quali: AFFIDABILITÀ (V.), DISPONIBILITÀ (V.), PRESTAZIONI (V.), sicurezza ecc. Tali requisiti sono quantificati dai contraenti e vengono misurati sulla base di indicatori concordati.

MAINFRAME
V. SISTEMI CENTRALI.

MINACCIA
Qualcosa di indesiderabile che potrebbe colpire con conseguenze negative un sistema. La *minaccia* può evolversi in RISCHIO (V.).

MIRRORING
Tecnica di scrittura dei dati in doppio (*dual-copy)* su due dispositivi fisici distinti, finalizzata al recupero delle informazioni in caso di guasto di uno dei due dispositivi (V. RAID).

MISURE DI CONTINGENCY
Interventi da porre in atto qualora, a causa di un DISASTRO (v.), non sia possibile ripristinare la funzionalità di una applicazione nel tempo massimo previsto. Tali misure sono tipicamente di tipo organizzativo e amministrativo e di norma prevedono il coinvolgimento dell'utente dell'applicazione. Le *misure di contingency* sono indicate nel BUSINESS CONTINGENCY PLAN (v.) dell'applicazione.

MISURE DI RECOVERY
Interventi da porre in atto per ripristinare nel tempo massimo previsto la funzionalità di una applicazione a seguito di INCIDENTE (v.), INCIDENTE GRAVE (v.) o SITUAZIONE DI CRISI (v.). In caso di necessità, e solo quando il problema sia di tipo infrastrutturale, la misura estrema è rappresentata dal DISASTER RECOVERY (v.). Le *misure di recovery* per ogni applicazione sono indicate nel BUSINESS CONTINUITY PLAN (v.).

NON RIPUDIO
Proprietà di non consentire alle parti in causa di disconoscere una transazione effettuata. Le tecniche di *non ripudio* si basano essenzialmente sulla FIRMA DIGITALE (v.).

OUTSOURCING (ESTERNALIZZAZIONE)
Acquisizione dall'esterno di un servizio di supporto all'Azienda. Può riguardare i sistemi informatici (gestione sistemi elaborativi e reti, HELP DESK (V.), fornitura apparati, sviluppo di applicazioni), le infrastrutture (manutenzione impianti, sorveglianza), la formazione, ecc..

PARALLEL SYSPLEX
Architettura dei SISTEMI CENTRALI (V.) IBM che si basa su un "complesso" formato da più elaboratori che colloquiano fra loro per consentire lo smaltimento del carico di lavoro. I sistemi (fino ad un massimo di 32) cooperano fra loro e condividono i dati. I sistemi possono anche essere

dislocati in siti distanti tra loro (con le tecnologie attuali non più di 20 km); in questi casi di parla di *Parallel Sysplex Distribuito* o G*eographically Dispersed Parallel Sysplex.*

PASSWORD
Parola d'ordine o stringa di caratteri che deve essere conosciuta solamente dal soggetto assegnatario per consentire la sua identificazione.

PIANO DI DISASTER RECOVERY
Documento nel quale sono comprese tutte le attività atte a effettuare il DISASTER RECOVERY (V.). Prende in considerazione problematiche hardware, software, di tipo logistico e organizzativo al fine di consentire la prosecuzione delle elaborazioni vitali dell'azienda.

PROCESSORE (CPU - CENTRAL PROCESSING UNIT)
Unità di controllo all'interno di un computer che gestisce le funzioni di elaborazione del sistema. Termine che identifica il microprocessore che costituisce il cuore della capacità elaborativa del computer.

PROTOCOLLO DI TRASMISSIONE
Insieme di regole alle quali devono uniformarsi i messaggi inviati sulle RETI DI TELECOMUNICAZIONE (V.) per consentire il colloquio tra elaboratori. Un protocollo si dice *proprietario* quando è utilizzabile solo per il colloquio tra apparati prodotti dalla stessa casa costruttrice (ad es. SNA è un protocollo *proprietario* della soc. IBM, utilizzabile con macchine prodotte dalla stessa IBM o interamente compatibili con queste). Viceversa un protocollo si dice *aperto* quando è utilizzabile con elaboratori diversi (ad esempio TCP/IP è un protocollo aperto utilizzabile da apparati IBM, Digital, Olivetti, ecc.).

RAID (REDUNDANT ARRAY OF INDEPENDENT DISKS)
Tecnologia che fornisce protezione contro la perdita di dati, basata sul concetto di "disco logico" indipendente dal supporto fisico. Il principio di funzionamento si basa su batterie di dischi *(disk array)* che, acceduti in parallelo, consentono una maggiore velocità di trasferimento dati. Vengono inoltre utilizzate delle *informazioni di parità* per ricostruire i dati in caso di guasto di dischi che compongono l'*array*.

Dal punto di vista teorico sono stati introdotti 6 livelli RAID, le cui caratteristiche principali possono essere così sintetizzate:
RAID1: Si tratta del cosiddetto MIRRORING (V.) o *dual-copy*: i dati vengono scritti in doppio su due dischi diversi.
RAID2: il dato viene frazionato in *unità* che vengono scritte (e lette) in parallelo su più dischi dell'array (*byte striping*). Viene introdotto anche il concetto di disco di controllo (*check disk*) per il recupero di situazioni di guasto o errore con una ridondanza di informazioni inferiore al caso precedente (ad esempio con 10 dischi dati sono necessari solo 4 dischi di controllo).
RAID3: rispetto al *raid2* riduce in modo significativo il numero di dischi di controllo basandosi sull'utilizzo di un bit di parità: viene utilizzato un singolo disco di controllo per ogni insieme di dischi dati.
RAID4: la singola operazione di lettura/scrittura interessa esclusivamente un solo disco dell'array (oltre il disco di parità). Vengono migliorate le prestazioni, in quanto il dato viene frazionato in unità più lunghe (*block striping*).

RAID5: le informazioni di parità sono distribuite sui dischi dati che a rotazione assumono anche funzioni di parità. In tal modo si rimuove il "collo di bottiglia" costituito dal singolo disco di controllo (acceduto da tutte le richieste di scrittura).
RAID6: innalza il livello di affidabilità tramite una doppia parità che consente all'*array* di continuare a funzionare anche in caso di guasto di due dischi.

RETE DI TELECOMUNICAZIONE
Insieme di mezzi per la trasmissione a distanza dei dati che può comprendere l'uso di linee telefoniche, di collegamenti via cavo, di collegamenti tramite satelliti geostazionari, ecc..

RISCHIO
MINACCIA (V.) che ha reali probabilità di colpire un sistema con impatti significativi. Una *minaccia*, qualora siano state adottate le opportune misure di protezione, non necessariamente costituisce un *rischio*.

RISERVATEZZA
Proprietà per cui un'informazione non è resa disponibile né è divulgata a entità, soggetti o processi non autorizzati.

ROUTER
Apparato utilizzato per l'interconnessione delle RETI DI TELECOMUNICAZIONE (V.).

SERVER
Sistema che viene utilizzato nell'ambito di APPLICAZIONI CLIENT/SERVER (V.). Tra le possibili funzioni che i *server* possono svolgere, si citano la gestione delle basi dati, le connessioni alla rete, l'autenticazione degli utenti, la gestione della posta elettronica, ecc..

SINGLE POINT OF FAILURE
Elemento di un sistema informatico, di una rete di telecomunicazione, di un impianto tecnologico, ecc. che, non disponendo di ridondanza, in caso di guasto comporta l'INDISPONIBILITÀ (V.) dell'intero sistema di cui fa parte.

SISTEMI CENTRALI (MAINFRAME)
Sistemi di grande capacità elaborativa e di memorizzazione delle informazioni, basati su tecnologie in grado di assicurare la massima DISPONIBILITÀ (V.), AFFIDABILITÀ (V.) e sicurezza. Per tali caratteristiche sono in genere utilizzati per le APPLICAZIONI VITALI (V.) dell'azienda.

SISTEMI INTERMEDI
Sistemi elaborativi di media potenza, destinati all'automazione di un settore aziendale (*sistemi dipartimentali*) o per utilizzi specializzati (SERVER (V.) di vario tipo, FIREWALL (V.), ecc.).

SITO DI DISASTER RECOVERY
Sito alternativo al CED (v.) da impiegare in caso di DISASTER RECOVERY (v.). Può essere dotato di dispositivi informatici (incluso o meno il software) o solamente di attrezzature logistiche (*empty shell)*. Di norma è ubicato in località fisica distinta rispetto al sito principale.

SITUAZIONE DI CRISI
Problema che ha impatto nei confronti degli utenti interni ed esterni all'azienda, che viene risolto nei tempi massimi previsti, eventualmente applicando idonee MISURE DI RECOVERY (v.).

SWITCH
Apparato di commutazione impiegato nelle reti locali.

TRACCE DI AUDIT
Registrazioni prodotte dal sistema operativo o, qualora previsto, dall'applicazione, per consentire di ricostruire la sequenza degli eventi significativi di una elaborazione. Tali registrazioni sono funzionali per la CONTROLLABILITÀ (V.) delle applicazioni o dei sistemi.

UNATTENDED
Sistema informatico o tecnologico non presidiato, in cui il controllo avviene a distanza, attraverso idonei strumenti e programmi di servizio.

UPS (UNINTERRUPTIBLE POWER SUPPLY)
Dispositivo basato su batterie di accumulatori, che consente di erogare energia anche in caso di abbassamento di tensione o interruzione temporanea dell'alimentazione elettrica.

VIRUS INFORMATICO
Componente software, redatto solitamente in linguaggio macchina, atto a provocare malfunzionamenti di varia natura più o meno dannosi all'operatività funzionale del sistema elaborativo e in grado di autoreplicarsi e autodiffondersi su altri sistemi anche attraverso i collegamenti trasmissivi. Benché qualunque sistema teoricamente possa essere soggetto ai *virus informatici*, in pratica il fenomeno si è sviluppato unicamente sui personal computer, data la capillare diffusione degli stessi e le protezioni relativamente deboli dei sistemi operativi di cui sono dotati.

7. BIBLIOGRAFIA

1) CIPA - *Gruppo di lavoro "Disaster Recovery"* - Maggio 1995.

2) ABI - *Y2K Progetto Anno 2000 - Piani di Contingency* - Giugno 1999.

3) ABI - *Rilevazione sullo stato della sicurezza* - 1998 (biennale).

4) Andrew Hiles, Peter Barnes - *The Definitive Handbook of Business Continuity Management* - John Wiley & Son Ltd; June 1999.

5) Kenneth L. Fulmer - *Business Continuity Planning: A Step-by-Step Guide (with Planning Forms & Diskette)* - Philip Jan Rothstein - January 1999.

6) Contingency Planning & Recovery Institute Consulting Staff - *500 Vital Points to Ensure Foolproof Contingency and Disaster Resumption Plans* - Management Advisory Publications - 1995.

7) Kenneth N. Myers - *Manager's Guide to Contingency Planning for Disasters: Protecting Vital Facilities and Critical Operations* - John Wiley & Sons - August 1999.

8) Contingency Planning & Recovery Institute Consulting Staff - *How to prepare Critical Business Process Contingency* - Management Advisory Publications - February 2000.

9) Laura G. Kaplan - *Emergency and Disaster Planning Manual* - McGraw Hill Text - February 1996.

10) Alan M. Levitt - *Disaster Planning and Recovery: A Guide for Facility Professionals* - John Wiley & Sons - April 1997.

11) Philip Jan Rothstein - *Disaster recovery testing: exercising your contingency plan* - Rothstein Associates - 1995.

12) Stephen Grey - *Practical Risk Assessment for Project Management* - John Wiley & Sons - June 1995.