Validazione di Piani di Disaster Recovery mediante Simulatore

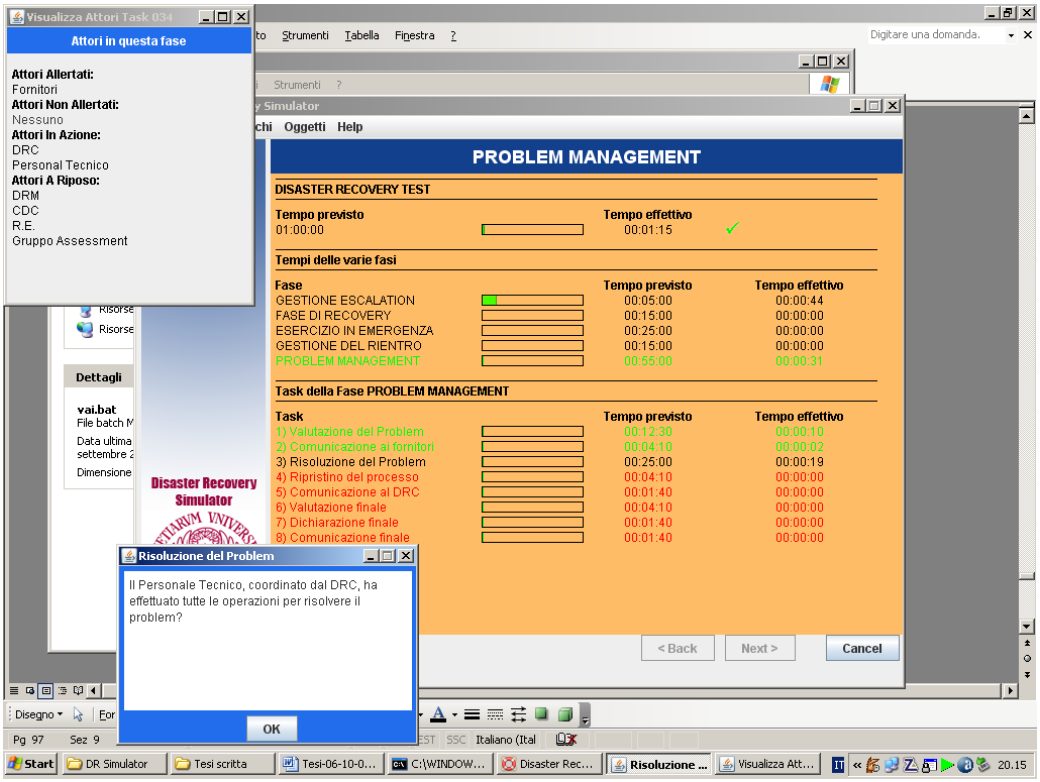
A.Cortesi, R.D'Orsi, F.Marcato, M.Peris, A.Sfoggia
Dipartimento di Informatica
Università Ca' Foscari Venezia

Il Business Continuity Plan è il piano che ogni azienda deve possedere per far fronte a qualsiasi tipo di imprevisto che potrebbe mettere in crisi la continuità operativa dell'azienda stessa. Esso viene usualmente considerato come un processo globale al cui interno risiede sia l'identificazione degli eventi che potenzialmente possono minare la sicurezza dell'organizzazione, che il metodo per fronteggiarli nel modo più accurato in modo di salvaguardare gli stakeholder, l'immagine e tutte le attività produttive dell'azienda stessa.
Un ruolo chiave all'interno del Business Continuity plan è costituito dal Piano di Disaster Recovery, che può essere inteso come il sottoinsieme delle attività atte al ripristino del sistema informatico dell'azienda e alla riattivazione in particolare di quei processi "business critical", che non possono rimanere bloccati.
A seconda della tipologia di azienda, i processi ICT possono essere di per se stessi determinanti per la continuità del business. Le componenti del sistema potranno essere classificate in funzione dell'impatto e della tolleranza all'indisponibilità delle stesse, dividendole in: critiche, vitali, delicate, non critiche. Ad un estremo, i sistemi critici sono quelli per i quali un'indisponibilità anche breve ha un impatto elevato e non possono essere sostituiti con procedure o strumenti alternativi. All'altro estremo, i sistemi non critici hanno un impatto limitato anche in caso di indisponibilità prolungata, e possono essere temporaneamente sostituiti, eventualmente, anche da procedure manuali.
Per quanto riguarda specificatamente il sistema ICT aziendale, un piano di Disaster Recovery dovrà prevedere la possibilità di riattivare i processi critici e vitali nel più breve tempo possibile. Al fine di rendere operativi tali interventi si rende necessario l'utilizzo di un sito remoto (o alternativo) dove poter intraprendere tutte le attività critiche aziendali.
In particolare, le aziende di credito già da alcuni anni sono chiamate a rispettare sia le normative ISO di qualità [6] che le raccomandazioni emesse dalla Banca d'Italia [2] atte a garantire la continuità del servizio verso la clientela. Misure più stringenti e specifiche sono inoltre richieste a livello internazionale [3,4].

Perché un piano di Disaster Recovery sia efficace risulta necessario procedere a simulazioni "reali" di eventi disastrosi, perché ciò consente, nel momento dell'effettiva occorrenza del disastro, di gestire in modo appropriato la sequenza di azioni previste. Ma prima ancora è necessario che sia verificata la consistenza delle assunzioni temporali e la compatibilità delle azioni previste, cosa che può essere facilitata dall'utilizzo di uno strumento di simulazione. Tale strumento può inoltre essere utilizzato non solo per l'addestramento del personale e per la evoluzione del sistema stesso, ma anche come strumento operativo, nel caso di disastro, per accompagnare e guidare le fasi di ripristino.

Sulla base delle norme specifiche della normativa BS 25999-2, che integra quanto richiesto dalla ISO 27001, abbiamo proceduto alla formalizzazione in UML [5] dei processi che sono richiesti per il piano di Disaster Recovery di una azienda di tipo finanziario (Gestione dell'Escalation., Gestione del Recovery, Gestione dell'Esercizio in Emergenza, Gestione del Rientro, Problem Management)., e sulla base di tale formalizzazione abbiamo realizzato un prototipo di simulatore generico per piani di Disaster Recovery, che può essere istanziato dando dei valori effettivi ai parametri associati ai diversi processi.

Il simulatore è stato sviluppato usando il linguaggio di programmazione Java. In particolare utilizza il package Swing di Java che dà la possibilità di creare programmi Java con interfaccia grafica. All'interno del simulatore sono stati creati cinque diversi documenti XML con i loro relativi DTD. Ogni documento risponde ad una particolare esigenza del simulatore: la lista degli oggetti, la lista dei processi, la lista dei rischi, la lista delle locazioni fisiche, la lista delle attività.
Particolare importanza si deve dare alla gestione delle planimetrie, che permettono di legare le strumentazioni, i processi ad esse associati ed il personale che vi opera, che devono essere gestite a runtime per seguire passo-passo l'evoluzione del sistema di ripristino.



Nella figura mostriamo il pannello del simulatore. All'interno della finestra principale vengono visualizzate informazioni relative al tempo totale del test, le varie fasi, i task della fase corrente e i relativi tempi. Per ogni fase e per ogni task è visualizzato il tempo previsto e il tempo effettivo e, per una miglior comprensione dello stato corrente della simulazione, accanto ad ogni voce è presente un rettangolo che andrà via-via riempiendosi (da verde a rosso) con il passare del tempo. Al di fuori della finestra principale sono presenti altre due finestre: una visualizza gli attori che partecipano al task corrente e il loro relativo ruolo (possono essere, difatti, attivi, a riposo, allertati o meno), mentre l'altro raffigura il task vero e proprio, che viene proposto in modo interattivo all'utente per procedere alle fasi successive.

Il programma proposto risulta essere un valido strumento a supporto della valutazione di un piano di Disaster Recovery. Permette infatti di evidenziare la congruità dei parametri utilizzati con le finestre temporali effettivamente disponibili nei diversi scenari associati agli eventi considerati. E' stato utilizzato per la validazione di uno specifico piano per una importante azienda finanziaria, che in vista del processo di certificazione a livello internazionale richiedeva una evidenza oggettiva di validità del proprio piano.

I risultati di questo progetto hanno contribuito alla realizzazione di un quaderno di guida alla gestione della continuità operativa edito dalla Associazione Italiana Cultura Qualità (AICQ) [1].

Riferimenti

[1] AICQ Triveneta, La Gestione della Continuità Operativa, Quaderno AICQ 28, 2008.

[2] Banca d'Italia, Linee Guida per la Continuità di Servizio delle Infrastrutture Qualificate dei Sistemi di Pagamento. 2004.

[3] BSI BS 25999-1 Business Continuity Management.A Code of Practice. 2006. (http://www.thebci.org/)

[4] BSI BS 25999-2 Business Continuity Management. Specification. 2007. (http://www.thebci.org/)

[5] Grady Booch, James Rumbaugh, Ivar Jacobson, The unified modelling language user guide, Addison Wesley, 1999.

[6] ISO/IEC 27001:2005, Security techniques information-security management systems – requirements. 2005.