DATA MANAGER

Mensile

Data 05-2014
Pagina 53
Foglio 1

speciale
outsourcing tecnologico

Dario Bonavitacola, responsabile della direzione
Infrastrutture Tecnologiche, Servizi e Sicurezza di Cedacri
(www.cedacri.it)

Le regole del rischio Le banche rivedono l'IT

La circolare 263 di Banca d'Italia impone agli istituti finanziari di rivedere le strutture IT deputate alla business continuity e al disaster recovery per innalzare la tutela dal rischio operativo

La circolare 263 del luglio 2013 è solo l'ultima di una serie che Banca d'Italia ha definito negli ultimi anni per rafforzare le misure di tutela delle banche rispetto al rischio operativo. Il documento mette in particolare evidenza i servizi IT fra gli elementi fondamentali su cui vigilare a tutela del rischio, andando così a delineare una serie di adeguamenti che le banche dovranno apportare ai propri sistemi informativi a garanzia della business continuity e del disaster recovery. È fondamentale che a tutte queste disposizioni rispondano pienamente anche gli outsourcer cui le banche scelgono di affidarsi per la gestione delle loro infrastrutture in questo ambito. Bisogna premettere che le nuove normative distinguono tra le banche che non creerebbero rilevanti squilibri alla normale operatività del Sistema Paese nel caso di problemi di operatività che dovessero interessarle, e quelle che invece offrono servizi di carattere sistemico, per via delle loro dimensioni o delle eventuali funzioni istituzionali che ricoprono. A quest'ultima categoria viene richiesta l'ottemperanza a un maggior numero di disposizioni, a salvaguardia del funzionamento del Paese nel suo complesso. Guardando agli outsourcer di servizi tecnologici, è auspicabile che essi si adeguino alle disposizioni imposte alle banche sistemiche, offrendo così un più alto livello di tutela ai propri clienti, anche in considerazione di eventuali future evoluzioni normative.

CLASSIFICAZIONE DEI SISTEMI IT - La Banca d'Italia ha innanzitutto introdotto l'obbligatorietà per tutti gli istituti di credito di sviluppare una classificazione dei sistemi IT in relazione alla maggiore o minore criticità per il business, distinguendo dunque le attività vitali per la banca da ciò che può essere considerato accessorio.

La circolare 263 impone inoltre una corretta organizzazione della funzione IT - in termini di persone, processi e procedure - volta a garantire la business continuity: si richiede dunque, a prescindere dai contenuti tecnici, che banche o outsourcer che prestano servizi informativi a queste ultime possiedano un documento esaustivo che descriva compiutamente l'approccio alla business continuity.

Tra le nuove regole imposte, quella forse più rilevante richiede che sussista una egual potenza elaborativa fra il sito di produzione e quelli di business continuity e disaster recovery: tutte le banche devono cioè essere in grado di erogare servizi di business continuity in una situazione di emergenza mantenendo gli stessi standard del servizio di produzione.

DISASTER RECOVERY - La circolare impone anche nuove disposizioni in merito alla localizzazione della struttura di disaster recovery, richiedendo che venga situata al di fuori delle aree metropolitane. Le normative non contengono però specifiche sulla distanza che deve intercorrere tra il sito e il centro urbano: si tratta di un aspetto attorno a cui è auspicabile si ottenga presto una maggiore chiarezza. Un'ulteriore accortezza in questo senso, che non figura nella circolare 263, ma che potrebbe ulteriormente innalzare il livello di tutela dal rischio, è la scelta di localizzare i siti produttivi e quelli di disaster recovery in aree geomorfologiche diverse: in questo modo, eventuali calamità naturali di forti dimensioni che dovessero coinvolgere un sito, più difficilmente avranno impatto anche sull'altro.

Se le indicazioni fin qui esaminate valgono per tutti i modelli di banca, agli istituti sistemici viene richiesta anche l'ottemperanza di altre due disposizioni. In primo luogo le banche sistemiche devono garantire - in caso di uno switch di disaster recovery - una ripartenza con il primo servizio IT entro due ore dal disastro e di ripristinare tutti i servizi critici entro quattro ore. L'altra richiesta che viene fatta alle banche sistemiche riguarda la resilienza dei lavoratori: le persone impiegate nella gestione dello switch di disaster recovery devono essere diverse da quelle che lavorano nel sito di produzione. Il secondo sito deve quindi operare in un regime di totale autonomia a livello del personale.

DM