

LINEE GUIDA PER LA CONTINUITA' DI SERVIZIO  
DELLE INFRASTRUTTURE QUALIFICATE DEI SISTEMI  
DI PAGAMENTO

## 1. INTRODUZIONE

Lo sviluppo tecnologico, la globalizzazione dei mercati finanziari, le conseguenti spinte competitive e le aggregazioni ancora in atto hanno modificato la struttura e l'operatività del sistema finanziario e, più in particolare, dei sistemi di pagamento. Tali cambiamenti hanno accresciuto i collegamenti e le interdipendenze tra i partecipanti ai sistemi e tra questi e gli altri operatori coinvolti nel loro regolare funzionamento, *in primis* i fornitori di servizi di infrastruttura. Il nuovo quadro di riferimento rende necessario assicurare non solo la capacità di ripristinare il servizio erogato in caso di guasti o malfunzionamenti, ma di garantire la continuità del servizio (*business continuity*).

L'attacco terroristico dell'11 settembre 2001 ha reso drammaticamente attuale la tematica della continuità di servizio: da allora si è intensificata l'azione delle Autorità e delle Banche Centrali per rafforzare il grado di resistenza dei sistemi finanziari ad eventi catastrofici. Obiettivi di fondo sono la minimizzazione del rischio sistemico, il ripristino in tempi brevi e l'integrità delle informazioni funzionali alla rapida ripresa della normale operatività sui mercati. A tali fini, è stata rimarcata l'esigenza di una programmazione e implementazione più sistematica dei piani di emergenza e della fissazione di concreti obiettivi di continuità di servizio per gli operatori rilevanti nonché della promozione di sedi di coordinamento per le iniziative di sistema. In alcuni paesi sono state emanate linee guida di orientamento per gli operatori di mercato.

Le analisi condotte hanno posto in luce il ruolo cruciale delle infrastrutture nel funzionamento dei moderni sistemi finanziari, sì da configurarle come il punto di maggiore concentrazione del rischio sistemico di natura operativa. Siffatta rilevanza è riconducibile alla fondamentale funzione da esse svolta nel trattamento delle operazioni finanziarie, attraverso la partecipazione, diretta o di supporto, alle fasi di compensazione e di regolamento. Ritardi o blocchi nell'attività delle stesse infrastrutture si ripercuotono direttamente su quella degli intermediari e dei mercati, al punto che la qualità del servizio offerto da questi ultimi viene, in buona misura, a dipendere da quella delle prime. Tale condizionamento si fa critico allorché, in situazioni di malfunzionamento esteso, non vi sono canali alternativi, facilmente attivabili per la esecuzione delle transazioni.

La Banca d'Italia ha avviato una serie di iniziative con la collaborazione delle infrastrutture, di mercato e dei sistemi di pagamento, e dei principali gruppi bancari, volte a rilevare lo stato di preparazione del sistema finanziario italiano a fronte di eventi della specie e a individuare, in apposita sede di coordinamento nazionale, le possibili linee di azione per ridurre le criticità a livello di sistema<sup>1</sup>. Ne risulta confermata la

---

<sup>1</sup> Si fa riferimento al Gruppo di lavoro, coordinato dalla Banca d'Italia d'intesa con la Consob, con la partecipazione delle strutture dell'Istituto maggiormente

crucialità del ruolo delle infrastrutture qualificate, assunte nel tempo a punti di significativa concentrazione operativa di rilevanti processi interbancari standardizzati.

Le presenti linee guida sono dirette, innanzitutto, a quelle infrastrutture qualificate che rilevano per la gestione e il controllo dei rischi in esame, così come definite nell'Allegato 1; nel futuro la Banca d'Italia potrà emanare specifiche linee guida per ulteriori fornitori di servizi di infrastruttura del sistema dei pagamenti nazionale, ovvero estendere a tali soggetti l'applicazione, in tutto o in parte, delle presenti linee guida, anche sulla base dell'attività di analisi condotta nell'ambito delle sedi di coordinamento nazionale.

Le linee guida trovano fondamento nelle previsioni, di cui all'art.146 TUB e del provvedimento del Governatore della Banca d'Italia del 24.2.04, volte ad assicurare il regolare funzionamento dei sistemi di pagamento nazionali. Esse forniscono i principi fondamentali cui vanno ispirati la predisposizione dei piani di continuità operativa e gli interventi, organizzativi e gestionali, atti a garantirne una piena attuazione in stretto raccordo con gli operatori di mercato.

## **2.Obiettivi**

Le infrastrutture qualificate che supportano il sistema dei pagamenti italiano possono essere distinte a seconda del livello di concentrazione o di standardizzazione dei servizi prestati, nonché della posizione assunta nel ciclo di perfezionamento dei diversi circuiti di pagamento. In particolare, l'elevato grado di standardizzazione delle procedure interbancarie realizzato nel sistema dei pagamenti nazionale ha avuto l'effetto di accentuare le interdipendenze tra tali infrastrutture e di posizionare le rispettive attività su basi operative contrassegnate da elevati livelli di omogeneità.

In ragione delle predette condizioni strutturali, nel concreto funzionamento operativo dei sistemi di pagamento nazionali emergono, pertanto, due fondamentali momenti di integrazione/interdipendenza: il primo, interno al comparto delle infrastrutture, e il secondo, come già sottolineato in precedenza, tra queste ultime e gli intermediari finanziari.

Ne discende che, nella predisposizione delle misure per contenere il rischio sistemico, a tali infrastrutture è richiesto un impegno particolare, commisurato al ruolo svolto nel sistema finanziario e coordinato con l'attività degli intermediari con cui interagiscono.

---

interessate al problema (Vigilanza sugli Enti Creditizi, Sorveglianza sul sistema dei pagamenti, Supervisione sui mercati, Sistema dei pagamenti, Elaborazione e sistemi Informativi, Segreteria CIPA), dell'ABI, dei principali gruppi bancari e delle infrastrutture rilevanti del sistema dei pagamenti e dei mercati.

Le presenti linee guida si ispirano a criteri di flessibilità, in grado di attivare un graduale e significativo processo di potenziamento dei presidi di continuità operativa, ancorato alla diversità degli scenari e dei relativi rischi assunti nonché all'esigenza di conseguire, nella realizzazione del citato processo, un rapporto ottimale costi/benefici. In tale ottica, è assegnata priorità massima ai servizi vitali ad elevato valore sistemico, così come appresso specificato. Inoltre, è fortemente raccomandato di coordinare al meglio, sulla base di una robusta pianificazione temporale, i necessari interventi di immediato potenziamento dei processi attuali con quelli, più incisivi, che potranno essere utilmente cadenzati nel tempo in connessione con revisioni strutturali indotte anche da altre esigenze di razionalizzazione delle procedure.

Un'attenta considerazione delle richiamate caratteristiche strutturali del sistema dei pagamenti nazionale può meglio orientare il processo decisionale in materia, soprattutto nella indicata modulazione temporale degli interventi richiesti. In particolare, l'elevato livello di standardizzazione dei servizi interbancari può rappresentare un'opportunità per l'adozione di soluzioni condivise da più operatori di sistema.

Le presenti linee guida si collegano a quelle emanate dalla Vigilanza e dalla Supervisione sui Mercati al fine di favorire le sinergie tra le infrastrutture qualificate, nonché fra queste e i maggiori intermediari e operatori finanziari, e di ottimizzare il rapporto costi/benefici dei singoli progetti.

### **3.La definizione e la gestione dei piani di continuità**

La definizione e la gestione del piano di continuità operativa costituiscono attività strategiche per le infrastrutture qualificate: come tali, esse richiedono, nella valutazione dei loro aspetti essenziali e nelle connesse scelte decisionali, il coinvolgimento diretto dei massimi organi amministrativi e di controllo.

In particolare, ricade nella responsabilità dei vertici aziendali la formulazione delle politiche in tema di continuità operativa e l'approvazione dei relativi piani di sviluppo e di gestione, ricercando il giusto equilibrio tra la minimizzazione degli investimenti e delle risorse da destinarvi e la capacità di resistenza dell'infrastruttura a rischi di ampia portata. A tali fini, il consiglio di amministrazione assicura, in coerenza con le indicazioni formulate nelle richiamate sedi di coordinamento nazionale, che nel piano stesso:

- a) siano chiaramente definite le attività vitali e critiche;
- b) siano assegnate le risorse necessarie per la realizzazione del piano;
- c) siano stabilite la frequenza e l'ampiezza delle verifiche periodiche (test e collaudi), comprensive di tutti i soggetti potenzialmente interessati;
- d) siano definite le priorità di ripartenza delle attività vitali e critiche in funzione delle esigenze delle controparti

- (Autorità, clienti, sedi di coordinamento nazionale) e dei vincoli esistenti a livello organizzativo e tecnologico;
- e) sia indicata la struttura dei collegamenti con i fornitori di servizi, con evidenza delle relative criticità;
  - f) siano previsti adeguati meccanismi per la valutazione degli interventi gestionali e dei risultati delle verifiche, con particolare riferimento agli effetti di natura sistemica, nonché per la promozione dei necessari interventi correttivi;
  - g) sia individuata la persona o la struttura incaricata di dichiarare lo stato di emergenza e chiaramente fissata la struttura di comando preposta alla gestione della crisi (alta direzione, comitato di crisi, gruppi interfunzionali, ecc.). In particolare, per le diverse tipologie di scenario, vanno puntualmente indicate le interconnessioni fra le diverse strutture coinvolte, le linee di riporto funzionale e le responsabilità connesse con l'espletamento delle attività da svolgere nei confronti dei partecipanti e dei delicati compiti di raccordo con le diverse autorità e le sedi di coordinamento nazionale.

Il consiglio riserva particolare attenzione alla previsione di adeguati meccanismi e procedure di controllo di pertinenza della funzione di revisione interna o di soggetti terzi indipendenti. In tale ambito, allo scopo di elevare l'affidabilità complessiva del piano, il consiglio stesso valuta attentamente le possibilità di applicazione di standard di sicurezza riconosciuti a livello nazionale e/o internazionale, nonché l'assoggettamento del piano stesso a valutazione da parte di terze parti ovvero a certificazione eseguita da laboratori di valutazione accreditati presso enti a ciò delegati, ove ciò fosse possibile in base agli standard di sicurezza prescelti. La certificazione del piano di continuità operativa può anche formare parte della più ampia certificazione dell'intero sistema di gestione della sicurezza delle informazioni.

La direzione partecipa a tutte le fasi più rilevanti del piano, assicurandone il rispetto ai diversi livelli di responsabilità. Essa attua le misure più idonee per diffondere la conoscenza del piano tra il personale; accerta che gli aspetti più importanti delle principali fasi del piano siano formalmente documentati; riferisce periodicamente agli organi amministrativi e di controllo sugli adempimenti previsti dal piano e sui relativi esiti.

### **3.1. La definizione dei piani di continuità**

La definizione dei piani operativi e il loro collegamento alle più generali politiche in tema di continuità di servizio deve far ricorso a metodologie consolidate, delle quali va assicurata adeguata conoscenza nei settori aziendali maggiormente coinvolti; nell'All. n.2 è riportato uno schema sintetico in linea con gli *standard* internazionali più diffusi.

Nella formulazione del piano devono trovare attenta e approfondita valutazione:

- gli scenari di rischio con le connesse analisi d'impatto;
- le soluzioni individuate riguardo alla localizzazione dei siti alternativi;

- le attività necessarie per il rispetto degli obiettivi di ripristino e ripartenza;
- le modalità di gestione e controllo del piano.

Decisiva, a tali fini, risulta la corretta e puntuale individuazione delle attività connesse con i servizi giudicati vitali e critici a livello di sistema.

**a. Servizi infrastrutturali vitali, critici, non critici.** La classificazione utilizzata tiene conto delle analisi condotte nelle sedi di coordinamento nazionale: essa si connette con la necessità di correlare gli interventi richiesti - con riguardo soprattutto ai tempi fissati per il ripristino e la ripartenza delle procedure - in funzione delle diverse esigenze di sistema e della loro scansione secondo ragionevoli criteri di priorità.

In termini generali, nell'area dei pagamenti sono considerati **vitali** quei servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco, anche di brevissima durata, ha rilevanti effetti negativi sull'operatività degli stessi (tipici, in questo ambito, i servizi di *clearing* e *settlement* dei pagamenti *wholesale*, cui di norma si connette un significativo rischio sistemico di regolamento). I servizi **critici** sono quelli che, pur assumendo particolare rilievo nell'attività dei diversi operatori, possono comunque tollerare, senza gravi inconvenienti, il blocco per alcuni giorni: in questo ambito possono collocarsi le principali procedure dei pagamenti *retail*, per le quali, in ragione di alcune caratteristiche strutturali del sistema dei pagamenti nazionale (ampio spessore ed elevata standardizzazione delle procedure interbancarie), si registra un significativo rischio sistemico di natura operativa per la marcata dipendenza dell'operatività degli intermediari da quella delle infrastrutture di sistema. I servizi **non critici** sono quelli non rientranti nelle due precedenti categorie.

Alla luce di tali principi, nella categoria dei servizi infrastrutturali **vitali** vanno ricompresi i servizi di regolamento lordo del contante (BIREL-TARGET) e di erogazione del contante tramite terminale ATM (Bancomat) nonché quelli di gestione delle infrastrutture telematiche di supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).

Per quanto riguarda il Bancomat, il servizio è ritenuto vitale a livello di sistema e non di singola banca. Le caratteristiche di circolarità del servizio, unitamente alla possibilità di utilizzo dello stesso "in aziendale", e l'attuale architettura applicativa, basata su una pluralità di strutture di supporto (autorizzative e di gestione dei terminali), rendono intrinsecamente robusto il servizio a fronte di indisponibilità dei singoli operatori. Va da sé che siffatta robustezza vale a condizione che non esistano informazioni o dispositivi che costituiscano un *single point of failure*, capace cioè di compromettere la funzionalità complessiva del servizio (per esempio: dipendenza da servizi di *utilities*, gestione accentrata di chiavi crittografiche, ecc.). E' necessario che le infrastrutture qualificate verifichino nel continuo la permanenza di tale condizione e che eventuali modifiche architetturali siano attentamente valutate anche negli aspetti qui considerati.

Le infrastrutture qualificate definiscono la mappa delle attività correlate alla erogazione dei servizi vitali e critici, con l'indicazione dei relativi collegamenti, interni ed esterni, in termini di condizionamenti operativi, logici e temporali.

**b. Scenari di rischio e relativi impatti sulle risorse.** Vanno attentamente considerati i diversi scenari di rischio compresi quelli relativi a disastri su larga scala, così come definiti nell'All.n.3 (*geografico, informatico, settoriale*). Per ciascuno

di essi va effettuata un'approfondita analisi d'impatto, in termini di soggetti coinvolti (operatori, mercati, infrastrutture), di processi interessati (procedure e sistemi informatici, processi operativi e organizzativi) e di interrelazioni con il mondo esterno (partecipanti nazionali ed esteri ai sistemi finanziari, *utilities*, utenti finali). A tale analisi va logicamente legata l'individuazione delle possibili soluzioni, con la distinta valutazione degli investimenti richiesti in risorse tecniche, umane e logistiche. Particolare attenzione va riservata alla indicazione delle tecniche di verifica (test e collaudi), da condurre periodicamente (almeno una volta l'anno) in modo coordinato a livello di sistema o di gruppi di operatori.

**c. Siti alternativi.** Con riferimento ai diversi scenari di rischio, gli organi decisionali valutano le soluzioni tecnico-organizzative economicamente più convenienti in funzione degli obiettivi di ripristino e ripartenza enunciati al punto seguente, con particolare riguardo alla disponibilità e all'allocazione di uno o più siti alternativi. Va attentamente valutata la necessità di porre questi ultimi a distanza adeguata dal sito primario per minimizzare la probabilità di blocco contemporaneo dei centri in caso di incidente e per assicurare il ripristino e la ripartenza delle procedure entro i tempi prestabiliti.

E' possibile il ricorso a modelli condivisi di gestione del sito alternativo (mutuo soccorso) tra due o più infrastrutture e/o intermediari ovvero a forme di *outsourcing* delle procedure di *recovery*. In entrambi i casi, vanno approntati adeguati meccanismi gestionali atti ad assicurare, nell'azione coordinata con i terzi fornitori di tali servizi, il rispetto sostanziale delle presenti linee guida.

Il vertice aziendale deve assicurarsi, sulla base di adeguate analisi, che i due siti - primario e alternativo - abbiano profili di rischio differenti e sottoporre ad attenta valutazione il rischio residuo di blocco contemporaneo degli stessi; in siffatta valutazione si tiene conto, tra l'altro, delle caratteristiche morfologiche del territorio e delle vie di comunicazione che collegano i due siti, delle relative architetture tecnologiche e della disponibilità sul territorio di fornitori alternativi.

Va attentamente valutata la definizione di misure di estrema emergenza per fronteggiare l'eventualità di un blocco contemporaneo dei centri primario e alternativo. In quest'ambito si inserisce la possibile attivazione di un terzo sito di *recovery*, anche attraverso adeguate forme di cooperazione con altri operatori e fornitori, nei casi in cui, per l'importanza della funzione svolta nell'ambito del funzionamento di un servizio "vitale" o "critico", risultino particolarmente rilevanti gli effetti di natura sistemica derivanti da un blocco simultaneo dei primi due.

Infine, è necessario approntare specifiche misure atte a contenere i rischi - come quelli di natura informatica (cfr. all. 3) - rivenienti da eventuali attacchi per i quali la stessa disponibilità di un sito alternativo non costituisce presidio efficace.

**d. Obiettivi di ripristino e ripartenza.** Gli obiettivi di ripristino e di ripartenza per le infrastrutture sono fissati in rapporto alla rilevanza e alle caratteristiche tecnico-procedurali dei servizi svolti, sulla base della richiamata classificazione degli stessi in vitali, critici e non critici e delle eventuali altre modalità operative che potranno essere definite nelle sedi di coordinamento nazionale.

Tali obiettivi sono definiti in termini di "tempo" e di "punto di ripristino" (rispettivamente, *RTO-recovery time objective* e *RPO-recovery point objective*); il loro rispetto si pone come condizione indispensabile per la piena e funzionale ripartenza delle procedure di sistema e, quindi, dell'operatività degli intermediari nei tempi per questi stabiliti dalle norme emanate dalla Vigilanza.

In relazione al fondamentale obiettivo di consentire la ripartenza dei servizi vitali entro breve tempo dal verificarsi dell'incidente (RTO), in modo da consentire la ordinata chiusura della giornata operativa e contabile, le infrastrutture qualificate dovranno assicurare tempi di ripristino e di ripartenza delle proprie attività coerenti con le esigenze del sistema finanziario e in linea con gli obiettivi individuati nelle sedi di coordinamento nazionale. In particolare, la ripartenza e il ripristino delle attività vitali devono essere assicurate entro le due ore dalla dichiarazione dello stato di crisi, secondo le priorità di ripartenza definite nel piano.

Gli obiettivi in termini di RTO e RPO, pur autonomi da un punto di vista logico, si presentano interrelati sul piano del loro concreto perseguimento, in ragione soprattutto dei vincoli/possibilità di natura tecnologica e/o infrastrutturale. Ad esempio, per i prelievi da ATM, stante l'importo contenuto delle transazioni, RTO potrebbe essere più stringente di RPO. Al contrario, in alcune procedure di trasferimento fondi - soprattutto di elevato importo - la disponibilità di sistemi alternativi basati su fax e telefono potrebbe allentare i vincoli da RTO e rendere più stressanti i termini di RPO, stante la necessità di preservare al massimo l'integrità delle transazioni.

Siffatte condizioni tengono conto, da un lato, delle fondamentali esigenze connesse con l'ordinata ripresa dell'attività finanziaria e, dall'altro, delle interdipendenze esistenti tra i diversi operatori, a livello nazionale e internazionale.

E' largamente riconosciuta, con esplicite prese di posizione nelle sedi internazionali, la necessità di posizionare il ripristino e la ripartenza dei servizi vitali nello stesso giorno di regolamento in modo da contenere gli oneri e i rischi connessi con la ritardata chiusura della giornata contabile.

Con riferimento al sistema *TARGET*, le linee fondamentali di gestione della *business continuity* in caso di disastro prevedono che: a) tutti i pagamenti siano trattati nella stessa giornata contabile in cui sono immessi nel sistema e che la giornata contabile si chiuda con un ritardo massimo di due ore; b) durante l'interruzione del servizio le Banche Centrali siano comunque in grado di trattare in modo sicuro un numero ridotto di pagamenti critici entro 30 minuti dalla ricezione dell'ordine; c) l'operatività sia ripristinata presso il sito secondario entro due ore (non includendo il tempo necessario per i processi decisionali).

Azioni di stimolo analoghe alle presenti linee guida sono svolte da parte dei competenti organismi internazionali nei confronti della SWIFT, quale fondamentale rete di interconnessione internazionale da cui dipende ormai in larga misura il funzionamento dei sistemi di pagamento dei diversi paesi, compresa l'Italia. Particolare attenzione è rivolta al rafforzamento delle

# BANCA D'ITALIA

---

misure di resistenza dell'infrastruttura nei casi estremi di blocco contemporaneo dei centri operativi, da realizzare attraverso soluzioni capaci di assicurare tempi ragionevolmente brevi di ripristino in condizioni di degrado accettabile.

Le infrastrutture qualificate dovranno altresì assicurare l'integrità dei dati trattati nell'espletamento del servizio (RPO), ponendo in essere adeguati presidi procedurali atti a contenere al massimo l'eventuale perdita dei dati stessi, tendenzialmente da limitare all'ultima transazione inviata da ciascuna controparte; a questo riguardo, vanno definiti appositi raccordi procedurali con le controparti per il ripristino manuale delle transazioni perse, adottando gli accorgimenti necessari a minimizzare il rischio di elaborazioni duplicate o errate.

Per gli altri servizi, diversi da quelli vitali, gli obiettivi di ripristino e di ripartenza si articolano, in termini meno stringenti, per fasce di priorità, in relazione ai vari scenari di rischio. In particolare, la ripartenza dei servizi critici deve comunque avvenire entro un tempo relativamente breve - tendenzialmente dell'ordine di una settimana - dall'evento catastrofico, coerentemente con le priorità definite nel piano e in linea con le condizioni fissate nelle sedi di coordinamento nazionale.

Ai fini del raggiungimento degli indicati obiettivi di ripristino e ripartenza, possono essere utilmente attivate azioni cooperative volte al potenziamento della disponibilità dei servizi vitali e critici, basato su una mirata revisione delle architetture applicative e degli accordi interbancari, che sfrutti l'elevato livello di standardizzazione delle procedure e le sinergie operative esistenti fra le infrastrutture qualificate e gli intermediari finanziari.

È necessario volgere l'attenzione agli aspetti critici, specie nel passaggio dal sito primario al secondario, in modo da eliminare tutte le possibili cause di degrado e contenerne, nel tempo e nell'intensità, gli effetti sui servizi erogati assicurando elevati livelli di servizio. Vanno attentamente valutate e predefinite le modalità operative per supplire all'eventuale degrado, allungando gli orari di operatività o limitando i volumi delle transazioni immesse dai partecipanti al sistema. A questo riguardo rileva l'adeguatezza dimensionale dei meccanismi di back-up rispetto all'esigenza di far fronte a una concentrazione delle transazioni. È parimenti necessario che, in vista di tali situazioni di degrado, siano approntati efficaci meccanismi di monitoraggio che prevedano, tra l'altro, adeguate forme di valutazione dei servizi offerti e di raccordo con i partecipanti.

Elementi fondamentali per la continuità operativa sono la integrità e la disponibilità delle informazioni, nonché dei servizi elaborativi e di comunicazione. Sono necessari meccanismi per acquisire e gestire regolarmente copie di riserva dei dati e del software. Le copie devono essere conservate presso siti remoti, anch'essi dotati di un adeguato livello di protezione fisica e ambientale, coerente con i presidi previsti per il sito primario. Più in particolare: a) le procedure di ripristino, accuratamente documentate e regolarmente collaudate, devono assicurare che in caso di necessità le copie siano disponibili in modo integro e tempestivo; b) l'affidabilità dei supporti di memorizzazione delle copie di emergenza deve essere regolarmente verificata; c) per le attività vitali e critiche devono essere conservate almeno tre "generazioni" di copie di riserva; d) le attività operative devono prevedere la registrazione di archivi di log; e) le procedure per la gestione di guasti devono prevedere sia l'analisi dei log, per assicurare che i guasti siano stati risolti in modo adeguato, sia la verifica delle misure correttive per assicurare

che i controlli in essere non siano stati compromessi e che gli interventi siano regolarmente autorizzati.

Nel caso in cui il disastro comporti un blocco dei servizi essenziali (trasporti, energia, telecomunicazioni, ecc.) ovvero si registri una situazione di gravi danni o di serio pericolo sul lato umano, è possibile che gli obiettivi sopra enunciati subiscano un adattamento, in via straordinaria, sulla base delle indicazioni fissate nelle sedi nazionali di coordinamento della crisi. Appare necessario che le infrastrutture qualificate prevedano adeguate soluzioni in grado di assicurare, anche in tale circostanza, la ripartenza e il ripristino delle proprie attività vitali entro breve tempo dal verificarsi dell'incidente (RTO) coerentemente con le priorità di ripartenza definite nel piano e nelle sedi di coordinamento della crisi. L'eventuale perdita di dati (RPO) dovrà essere contenuta indicativamente entro le quattro ore precedenti la dichiarazione dello stato di crisi e dovranno essere predisposti adeguati meccanismi procedurali, atti a consentire la tempestiva ripresa delle transazioni perse e a minimizzare il rischio di elaborazioni duplicate o errate.

Le analisi condotte a livello internazionale e dal citato gruppo di lavoro, pongono in evidenza che il ricorso a soluzioni di estrema emergenza, per loro natura non completamente automatizzate, incontra limiti obiettivi di tempo in termini di utilizzabilità e sopportabilità da parte degli operatori. La gravità degli impatti sugli operatori tende a essere particolarmente onerosa se il blocco supera le 24/48 ore. Per tali ragioni, è importante che sia prevista la ripartenza, la più immediata possibile, delle procedure a supporto delle transazioni considerate irrinunciabili, sia pure con una funzionalità inizialmente ridotta e via via riportata a livelli di normalità; in ogni caso, anche le citate soluzioni di emergenza devono essere adeguatamente presidiate dal punto di vista della sicurezza.

### **3.2.La gestione e il controllo dei piani di continuità.**

Nella strategia complessiva volta a innalzare i livelli di resistenza delle infrastrutture ad eventi di tipo catastrofico e, più in generale, a tenere su livelli elevati la continuità operativa delle stesse, particolare attenzione va attribuita alle fasi di gestione e controllo dei piani, quali momenti essenziali per assicurare la piena ed efficace attuazione delle misure previste al verificarsi delle situazioni critiche.

Nella loro concreta espressione, tali attività si configurano come un complesso processo interattivo che si sviluppa dinamicamente sia nell'ambito aziendale, con forte interessamento delle variabili critiche della struttura (personale, risorse tecniche *hardware* e *software*, procedure operative, meccanismi di coordinamento organizzativo) sia nei rapporti con terzi. In mancanza di una chiara pianificazione e di un attento monitoraggio di questi aspetti, l'efficacia delle misure previste dal piano rischia di risultare vanificata completamente o parzialmente.

Momenti fondamentali di questo processo sono rappresentati da un'efficace e chiara azione di documentazione delle linee essenziali del piano di continuità e dalla sua diffusione all'interno dell'azienda attraverso un'adeguata attività di formazione e addestramento.

# BANCA D'ITALIA

---

Siffatti interventi rappresentano un presupposto indispensabile per favorire la condivisione degli obiettivi, ai diversi livelli di responsabilità, da parte delle strutture operative e per creare nel personale coinvolto la piena consapevolezza del proprio ruolo e l'esperienza necessaria a poter correttamente operare nelle situazioni di crisi ipotizzate.

E' essenziale che a tali aspetti siano riservate la massima attenzione e le risorse necessarie; l'effettuazione delle previste sessioni di test e collaudo deve costituire anche un momento importante di verifica del grado di preparazione del personale e della validità dei meccanismi gestionali approntati per il governo delle emergenze.

E' necessario che, nelle diverse fasi di realizzazione e controllo del piano, si proceda all'oggettiva rivelazione delle carenze e delle anomalie manifestate, i cui aspetti di rilievo vanno sottoposti alle valutazioni dei massimi organi amministrativi e di controllo. In tale ambito, l'esigenza di riallocazione di elementi chiave del personale deve essere minima e, ove inevitabile, la procedura di riallocazione deve essere chiaramente definita. E' preferibile che il sito primario e quello alternativo si avvalgano di diverse compagini.

Parimenti, di cruciale rilievo è la funzione che le infrastrutture qualificate devono svolgere nei confronti sia degli operatori (intermediari e altre infrastrutture) partecipanti ai sistemi da esse gestiti sia delle Autorità, anche in considerazione delle esigenze di comunicazione.

Nei rapporti con i partecipanti vanno assicurati adeguati meccanismi di coordinamento basati su: a) l'esplicitazione delle principali caratteristiche delle procedure di continuità di servizio e delle loro eventuali successive modifiche, con chiara evidenza dei punti di raccordo di particolare criticità; b) l'indicazione delle misure e delle cautele che ciascuna parte deve adottare per prevenire malfunzionamenti nell'operatività reciproca e ricadute di natura sistemica; c) la previsione di test e collaudi da svolgere periodicamente (almeno una volta l'anno) in modo integrato e congiunto; d) l'attivazione di punti di contatto da rendere disponibili nei casi di necessità e di crisi.

Nei confronti dei fornitori esterni, soprattutto rispetto alle società che erogano servizi essenziali per il funzionamento delle infrastrutture, sono da valutare e realizzare meccanismi e accorgimenti di natura logistica in grado di diversificare le fonti di approvvigionamento di tali servizi e di stabilire livelli di servizio predeterminati. La conoscenza delle priorità di ripristino del servizio che il fornitore attribuisce ai diversi clienti costituisce un elemento di valutazione circa l'affidabilità del medesimo in caso di crisi.

La concreta verifica dell'efficacia dei meccanismi di coordinamento costituisce un fattore di cruciale importanza ai fini del perseguimento di obiettivi di massima affidabilità dei sistemi finanziari in situazioni di emergenza. E' essenziale una puntuale e corretta esecuzione dei test e collaudi alle scadenze previste, atte a verificare la connettività tra i rispettivi siti primari e alternativi.

Le verifiche globali dei piani di emergenza devono simulare condizioni operative e volumi di attività realistici, effettuando il controllo delle funzionalità e delle prestazioni in situazioni di crisi e verificando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano. Il collaudo integrato ha lo scopo di coinvolgere anche i clienti/utenti e le controparti rilevanti e in tale fase va anche attentamente verificata l'adeguatezza della struttura dei collegamenti con i fornitori di servizi

# BANCA D'ITALIA

---

essenziali, simulando blocchi nell'erogazione degli stessi in modo da individuare le misure più appropriate per assicurarne la tempestiva rimozione o il superamento.

I risultati delle verifiche sono adeguatamente documentati, portati all'attenzione dell'alta direzione e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di *auditing*. A fronte di carenze riscontrate nelle prove l'infrastruttura avvia tempestivamente le opportune azioni correttive.

Più in generale, alle infrastrutture qualificate incombe l'onere - con un peso correlato alla posizione occupata nel funzionamento dei diversi circuiti finanziari - di avere un ruolo attivo verso i diversi operatori coinvolti, assumendo ogni iniziativa atta, da un lato, a rimuovere gli ostacoli alla regolare attuazione dei piani e, dall'altra, a promuovere comportamenti coerenti con tale obiettivo.

Parallelamente, proprio in virtù di tale posizione, le infrastrutture qualificate sono tenute a rappresentare alla Banca d'Italia le principali iniziative assunte in materia e, comunque, ogni circostanza o fatto che riduce il grado di affidabilità del sistema nel suo insieme o di parti rilevanti dello stesso. Inoltre, dovranno essere immediatamente segnalate le anomalie aventi ricadute significative sul livello di servizio offerto e i relativi interventi correttivi.

\*\*\*\*\*

I piani di continuità delle infrastrutture qualificate dovranno essere approntati e comunicati alla Banca d'Italia entro la fine del 2004. La realizzazione degli interventi previsti nei piani dovrà essere completata entro il 2006; semestralmente dovranno essere forniti riferimenti sullo stato di avanzamento dei lavori e sul livello di convergenza verso gli obiettivi di ripristino e ripartenza enunciati al cap. 3.1.d. In stretto raccordo con le conclusioni raggiunte nell'ambito dei lavori condotti nelle richiamate sedi di coordinamento nazionale, vanno prioritariamente analizzati e definiti i tempi di ripristino e di ripartenza per i servizi vitali e critici, da rendere noti alle diverse controparti.

Roma, 4 novembre 2004

## Allegato n.1

### DEFINIZIONI

**Infrastrutture qualificate:** infrastruttura valutata tale dalla Banca d'Italia in base alle previsioni di cui al Regolamento del 24.2.2004 di attuazione dell'art. 146 TUB (artt. 1, 4.2). Ai fini delle presenti linee guida, esse ricomprendono la SIA e i Centri Applicativi Interbancari Standardizzati.

**Disastro su larga scala:** è definito tale l'evento che causa una grave distruzione dei sistemi di trasporto, telecomunicazione, erogazione dell'energia o di altre infrastrutture in un'area metropolitana o più estesa; esso può condurre a disporre l'evacuazione o determinare l'inaccessibilità delle zone comprese in un determinato raggio dal luogo dell'evento.

**Piano di continuità operativa** (denominato anche **piano**): è il documento che in modo organico stabilisce, in stretto raccordo con gli obiettivi e le priorità aziendali, le regole per la gestione della continuità operativa dei diversi processi in caso di disastro su larga scala. Esso è articolato in più parti, tra loro coordinate, ciascuna riferita a un particolare settore, di rilievo per l'attività aziendale.

**Ripristino:** ricostruzione e sistemazione del pregresso (transazioni disposte dagli intermediari e non giunte a conclusione) dopo il disastro su larga scala. Si pone come condizione indispensabile per la piena ripartenza dell'operatività nei mercati.

**Ripartenza:** momento, successivo al disastro su larga scala, a partire dal quale è ristabilita la capacità di eseguire nuove transazioni, attivare i servizi a disposizione del cliente e chiudere la giornata contabile.

**Rischio Sistemico (di regolamento):** rappresenta il rischio che un partecipante a un sistema di pagamento o a mercati finanziari, non in grado di regolare le proprie obbligazioni, determini significativi problemi di liquidità o di credito ad altri partecipanti con effetti a catena in grado di minacciare la stabilità del sistema finanziario.

**Rischio Sistemico (di natura operativa):** rappresenta il rischio che un partecipante a un sistema di pagamento o a mercati finanziari, non in grado di eseguire o ricevere operativamente le proprie transazioni, determini significativi problemi operativi e/o di corretta determinazione delle posizioni contabili ad altri partecipanti con effetti a catena in grado di minacciare il regolare funzionamento del sistema finanziario.

**Punto di Ripristino** (*recovery point objective* - RPO): indica l'istante di consolidamento dei dati fino al quale è garantita l'integrità degli stessi.

**Tempo di Ripristino** (*recovery time objective* - RTO): rappresenta il massimo tempo di indisponibilità di un servizio o, in altri

termini, la velocità con la quale è necessario ripristinare il servizio fermo.

### I PIANI DI CONTINUITA' OPERATIVA

I piani di continuità operativa vengono formulati con riferimento a ciascuno dei servizi infrastrutturali definiti **vitali e critici**. Vanno assicurati, da un lato, il raccordo di tali piani con le più generali politiche aziendali in tema di continuità di servizio (**policy per la continuità operativa**) e, dall'altro, l'adozione di idonei meccanismi tecnico-organizzativi di coordinamento e di integrazione tra gli stessi, con particolare riguardo alle dipendenze reciproche (tempi e condizioni).

Gli standard internazionali più diffusi in materia indicano, nelle seguenti parti logiche, gli elementi fondamentali dei piani di continuità operativa<sup>2</sup>.

#### 1. Analisi d'impatto:

- analisi di impatto, in relazione agli scenari di rischio individuati e alla probabilità degli eventi considerati;
- individuazione delle macrosoluzioni e valutazione della relativa fattibilità economica (analisi costi/benefici).

#### 2. Controlli preventivi:

- Individuazione dei possibili presidi, di natura tecnico-organizzativa, di supporto ai piani di continuità e atti a ridurre o annullare l'impatto di determinati eventi (quali ad esempio: sistemi di continuità, ridondanza di impianti di condizionamento per le sale macchine; conservazione in sito remoto dei supporti di back-up e dei documenti cartacei più importanti, ecc.).

#### 3. Procedure di ripristino e ripartenza:

- individuazione e definizione delle procedure e delle varie fasi per il ripristino e la ripartenza nei tempi previsti delle attività considerate;
- descrizione delle caratteristiche dei siti alternativi e dei metodi di backup;
- valutazione delle dipendenze interne ed esterne, rilevanti per l'attivazione delle fasi di ripristino e ripartenza (obblighi contrattuali dei fornitori, compatibilità dei relativi metodi di backup, ecc.).

#### 4. Manutenzione, revisione e collaudo:

---

<sup>2</sup> I contenuti del presente allegato si richiamano ai principi e alle metodologie dei seguenti documenti :

- ISO/IEC 17799:2000(E) - information technology, code of practice for information security management - capitolo 11, business continuity management.
- NIST special publication 800-34; contingency planning guide for information technology systems, June 2002.

- definizione delle procedure per l'aggiornamento (manutenzione e revisione) dei piani al verificarsi di fatti modificativi (acquisizione di nuovo hardware; modifica dei sistemi operativi; cambiamenti del personale; eventi esterni che hanno riflessi sul piano, ecc.);
- definizione delle procedure per la realizzazione periodica del collaudo del piano e dei test integrati (periodicità; cadenza, modi e tempi di esecuzione delle diverse fasi; modalità di raccordo con i partecipanti e con gli altri sistemi);
- previsione di meccanismi formali per l'evidenziazione e per il reporting alla Direzione delle anomalie rilevate.

## **5. Misure di gestione:**

- previsione di corsi formativi periodici ai diversi livelli sul funzionamento dei piani nonché di meccanismi organizzativi di sensibilizzazione al problema;
- simulazioni di situazioni di crisi che impattano sulla singola procedura ovvero sull'intera infrastruttura;
- adozione di una metodologia adeguata per la documentazione delle procedure.

### SCENARI DI RISCHIO

Sulla base delle prime risultanze degli approfondimenti operati, con la collaborazione dei principali intermediari e delle infrastrutture qualificate, sono considerati fondamentali nella definizione dei piani operativi i seguenti tre scenari di rischio a valenza catastrofica:

- 1. di natura geografica:** riguarda l'indisponibilità di aree geografiche che, per l'elevata concentrazione dei principali intermediari e/o infrastrutture, risultino di particolare rilevanza per la regolare operatività del sistema finanziario nazionale. L'indisponibilità implica la difficoltà di accesso alle attività svolte in tali aree - costituite, di norma, dai principali centri metropolitani o da estensioni maggiori - a prescindere dalle cause sottostanti (fenomeni naturali, problemi di natura tecnologica, attacchi terroristici).
- 2. di natura informatica:** ricomprende gli attacchi di tipo informatico (penetrazione di sistemi, virus, *denial of service*, perdita della riservatezza, manipolazione di dati, etc.) perpetrati su siti ove risiedono le attività vitali di uno o più operatori rilevanti, tali da compromettere il normale ricorso ai sistemi di *recovery*.
- 3. di natura settoriale:** riguarda l'indisponibilità di singoli operatori rilevanti, conseguente al verificarsi di un evento disastroso, con effetti significativi sul resto del sistema.