BANCA D'ITALIA
EUROSISTEMA

MISURE DI CONTINUITÀ OPERATIVA

Allegato del Provvedimento della Banca d'Italia del 9 novembre 2021

INDICE

PREMESSA **3**

1 DEFINIZIONI **3**

2 MISURE DI CONTINUITÀ OPERATIVA **4**

2.1 Piano di continuità operativa **4**

2.2 Analisi di impatto **5**

2.3 Definizione del piano di continuità operativa e gestione delle crisi **5**

2.3.1 Ruolo degli organi aziendali ***5***

2.3.2 Processi critici ***6***

2.3.3 Responsabilità del piano di continuità operativa ***6***

2.3.4 Contenuto del piano di continuità operativa ***6***

2.3.5 Verifiche ***7***

2.3.6 Risorse umane ***7***

2.3.7 Ricorso a soggetti terzi per la prestazione di servizi ICT o per l'esternalizzazione, infrastrutture e controparti rilevanti ***8***

2.3.8 Controlli ***8***

2.3.9 Comunicazioni alla Banca d'Italia ***8***

2.4 Aspettative ulteriori della funzione di sorveglianza della Banca d'Italia in proporzione al rischio **9**

Definizione del piano di continuità operativa e gestione delle crisi ***9***

(a) Scenari di rischio ***9***

(b) Siti alternativi ***9***

(c) Tempi di ripristino e percentuali di disponibilità ***9***

(d) Risorse ***10***

(e) Verifiche ***10***

(f) Partecipazione al Codise ***10***

Premessa

Il presente allegato al Provvedimento della Banca d'Italia del 9 novembre 2021, recante Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete (di seguito Provvedimento), definisce un quadro di riferimento per le misure di continuità operativa che devono essere adottate dai gestori di sistemi di pagamento e dai fornitori critici di infrastrutture o servizi tecnici. Esso è costituito da due sezioni, riguardanti, rispettivamente, le definizioni dei principali termini usati e le misure di continuità operativa che i gestori di sistemi di pagamento e i fornitori critici di infrastrutture o servizi tecnici devono adottare (di seguito anche "gli operatori"), avuto riguardo alla dimensione, alla complessità operativa, al profilo di rischio e alle specificità delle attività svolte e dei servizi offerti[1].

Gli operatori si uniformano alle previsioni di cui al presente allegato e possono adottare le misure alternative ritenute adeguate, fornendone motivazione circostanziata in occasione delle comunicazioni periodiche alla Banca d'Italia (principio del *comply or explain*).

1 Definizioni

- "Codise (continuità di servizio)": struttura per il coordinamento delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia;
- "crisi": situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici in seguito a incidenti o catastrofi;
- "escalation": conduzione della gestione di un incidente caratterizzata da un aumento progressivo dei livelli aziendali coinvolti, fino a giungere, ove necessario, all'organo di amministrazione;
- "emergenza": situazione originata da incidenti o catastrofi che colpiscono l'operatore, caratterizzata dalla necessità di adottare misure tecniche e gestionali eccezionali, finalizzate al tempestivo ripristino della normale operatività;
- "gestione della continuità operativa": insieme delle iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti o catastrofi che colpiscono direttamente o indirettamente un operatore;
- "piano di continuità operativa": documento che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse per la gestione della continuità operativa dei processi aziendali critici. Esso è generalmente articolato in piani settoriali;
- "piano di *disaster recovery*": documento che stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino l'indisponibilità dei centri di elaborazione dati. Il piano di *disaster recovery*, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti anche in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa;
- "processi critici": processi - identificati dagli operatori - relativi a funzioni aziendali di particolare rilevanza che, per l'impatto dei danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa da conseguire mediante misure di prevenzione e con soluzioni di continuità operativa da attivare in caso di incidente;
- "punto di ripristino": istante di salvataggio dei dati fino al quale è garantita l'integrità degli stessi nei siti primari e alternativi;
- "sito alternativo": infrastruttura che consente all'operatore di continuare a svolgere i processi critici, anche in caso di incidenti o disastri che rendano indisponibile il sito primario;
- "sito primario": infrastruttura presso la quale di norma sono svolte le attività dell'operatore;
- "tempo di ripristino di un processo (*recovery time objective*, RTO)": periodo che intercorre fra il momento in cui l'operatore dichiara lo stato di crisi e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:
    - analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;

[1] Vedi anche l'art. 11 del Provvedimento.

- ripartenza del processo, attraverso l'attuazione degli interventi tecnici e organizzativi e la successiva verifica sulla possibilità di rendere nuovamente disponibili i servizi senza danni e in condizioni di sicurezza.

2 Misure di continuità operativa

Al fine di assicurare il regolare funzionamento del sistema dei pagamenti, nel suo complesso e nelle sue singole componenti, a tutti i gestori di sistemi di pagamento e i fornitori critici di infrastrutture o servizi tecnici sorvegliati ai sensi del Provvedimento è richiesto di adottare un insieme minimo di misure di continuità operativa.

La Banca d'Italia, in ragione del ruolo e del contributo di ciascuno degli operatori rispetto al funzionamento del sistema finanziario nazionale, definisce le modalità del loro coinvolgimento nelle attività del Codise in materia di continuità operativa del settore finanziario italiano.

2.1 Piano di continuità operativa

Gli operatori definiscono un piano di continuità operativa per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale ovvero a catastrofi estese che colpiscono l'operatore o le sue controparti rilevanti (altre società del gruppo; principali soggetti terzi che prestano servizi anche in regime di esternalizzazione; clientela primaria; specifici mercati finanziari, sistemi di regolamento, compensazione e garanzia).

I piani di continuità operativa prevedono soluzioni basate su misure tecnico-organizzative atte alla salvaguardia degli archivi elettronici e al funzionamento dei sistemi informativi, e che considerino anche ipotesi di crisi estesa e blocchi prolungati delle infrastrutture essenziali, in modo da assicurare la continuità operativa dell'operatore in simili circostanze. Laddove alcuni processi critici siano svolti da soggetti specializzati appartenenti al gruppo (ad es., società strumentali che gestiscono la funzione informatica o il back-office), le relative misure di continuità operativa costituiscono parte integrante dei piani degli operatori.

Il piano di continuità operativa si inquadra nella complessiva politica di governo dei rischi dell'operatore; il piano tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali. Il piano è documentato, messo a disposizione delle unità operative e di supporto e immediatamente accessibile in caso di emergenza. Inoltre, esso è rivisto con cadenza almeno annuale e aggiornato, laddove necessario, sulla base dei risultati delle verifiche, delle informazioni sulle minacce esistenti e dell'esperienza maturata in occasione di eventi precedenti[2]. Si veda anche il paragrafo 3.3 (Responsabilità del piano di continuità operativa).

Il piano prende in considerazione diversi scenari di crisi - incluso almeno uno scenario di attacco informatico - e considera almeno i seguenti fattori di rischio, conseguenti a eventi naturali o ad attività umana, inclusi danneggiamenti gravi da parte di dipendenti:

- Distruzione, inagibilità parziale o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di sistemi informativi critici;
- indisponibilità di personale essenziale per il funzionamento dei processi aziendali;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione o perdita di dati e documenti ritenuti critici.

[2] Nell'aggiornamento dei piani di continuità operativa, per i profili ICT gli operatori tengono conto anche delle modifiche degli obiettivi di ripristino (vedi par. 2.3.2), delle funzioni aziendali, dei processi di supporto e delle risorse informatiche.

Il piano indica le procedure per il rientro dall'emergenza, con particolare attenzione alla rilevazione degli impatti, alla gestione di tutte le operazioni di rientro, alla verifica della corretta disponibilità dei servizi ripristinati.

2.2 Analisi di impatto

L'analisi di impatto (*Business Impact Analysis*, BIA), preliminare alla stesura del piano di continuità operativa e aggiornata periodicamente[3], individua il livello di rischio relativo ai singoli processi aziendali sulla base di un approccio quantitativo e qualitativo, e pone in evidenza le conseguenze dell'interruzione del servizio. I rischi residui, non gestiti dal piano, sono documentati ed espressamente accettati dagli organi aziendali competenti.

L'allocazione delle risorse e le priorità di intervento sono correlate al livello di rischio.

L'analisi di impatto tiene conto dei parametri caratteristici della struttura organizzativa e dell'operatività aziendale, tra cui:

- le specificità – in termini di probabilità di catastrofe – connesse con la localizzazione dei siti rilevanti (ad es., sismicità dell'area, rischi di dissesto idrogeologico del territorio, vicinanza ad insediamenti industriali pericolosi, prossimità ad aeroporti o a istituzioni con alto valore simbolico);
- i profili di concentrazione geografica (ad es., presenza di una pluralità di operatori nei centri storici di grandi città);
- la complessità dell'attività tipica o prevalente e il grado di automazione raggiunto;
- le dimensioni aziendali e l'articolazione territoriale dell'attività;
- il livello di esternalizzazione di funzioni rilevanti (ad es., outsourcing del sistema informativo o del back-office) e il livello di ricorso a soggetti terzi per la prestazione di servizi ICT;
- l'assetto organizzativo in termini di accentramento o decentramento di processi critici;
- i vincoli derivanti da interdipendenze, anche tra e con soggetti terzi che prestano servizi anche in regime di esternalizzazione, clienti, altri operatori.

L'analisi di impatto prende in considerazione, oltre ai rischi operativi, anche gli altri rischi (ad es., di mercato e di liquidità).

2.3 Definizione del piano di continuità operativa e gestione delle crisi

2.3.1 Ruolo degli organi aziendali

Il tema della continuità operativa è adeguatamente valutato a tutti i livelli di responsabilità. In tale ambito, l'organo di amministrazione:

a) stabilisce gli obiettivi e le strategie di continuità operativa del servizio;
b) assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati;
c) approva il piano di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici ed organizzativi, accettando i rischi residui non gestiti dal piano stesso;
d) è informato, con frequenza almeno annuale, sugli esiti dei controlli sull'adeguatezza del piano nonché delle verifiche delle misure di continuità operativa;
e) nomina il responsabile del piano;
f) promuove lo sviluppo, il controllo periodico del piano ed il suo aggiornamento in presenza di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti;

[3] L'analisi di impatto ed i conseguenti piani per la continuità operativa sono rivisti annualmente e aggiornati sulla base di quanto appreso dalle verifiche effettuate, dall'individuazione di nuovi rischi e minacce, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino.

g) approva il piano annuale delle verifiche delle misure di continuità operativa ed esamina i risultati delle prove documentati in forma scritta.

L'organo con funzione di controllo ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del piano di continuità operativa.

L'attività svolta e le decisioni assunte sono adeguatamente documentate.

2.3.2 Processi critici

Gli operatori identificano in modo circostanziato - e comunicano alla Banca d'Italia - i processi relativi a funzioni aziendali di particolare rilevanza che, per l'impatto dei danni conseguenti alla loro indisponibilità, necessitano di livelli elevati di continuità operativa, da conseguire mediante misure di prevenzione e con soluzioni di continuità operativa da attivare in caso di incidente.

A tal fine, sono considerati con particolare attenzione i processi che attengono alla gestione dei rapporti con la clientela, ivi incluse imprese e pubbliche amministrazioni, e alla registrazione dei fatti contabili.

Per ciascun processo critico sono individuati il responsabile, le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate e le infrastrutture tecnologiche e di comunicazione utilizzate.

Il responsabile del processo individua, in accordo con gli indirizzi strategici e con le regole stabilite nel piano di continuità operativa, il tempo di ripristino del processo (*recovery time objective*, RTO) e il punto di ripristino prefissato (*recovery point objective*, RPO) e collabora attivamente alla realizzazione delle misure di continuità operativa.

2.3.3 Responsabilità del piano di continuità operativa

Il responsabile del piano di continuità operativa aziendale ha una posizione gerarchico-funzionale adeguata. Il responsabile cura lo sviluppo del piano di continuità operativa, ne assicura l'aggiornamento nel continuo, a fronte di cambiamenti organizzativi o tecnologici rilevanti, e ne verifica l'adeguatezza, con cadenza almeno annuale. Tiene inoltre i contatti con la Banca d'Italia in caso di crisi.

Se il piano di continuità operativa è articolato in piani settoriali gli operatori individuano i referenti per ciascuno di essi. I referenti dei piani settoriali[4] coordinano, per gli aspetti di competenza, i lavori per la definizione e la manutenzione dei piani, per l'attuazione delle misure previste nel piano di continuità operativa e per la conduzione delle verifiche. Prima dell'attivazione di nuovi sistemi o processi operativi, i suddetti referenti definiscono le opportune modifiche dei piani.

2.3.4 Contenuto del piano di continuità operativa

Il piano di continuità operativa documenta i presupposti e le modalità per la dichiarazione dello stato di crisi, l'organizzazione e le procedure da seguire in situazione di crisi, l'iter per la ripresa della normale operatività.

Il piano attribuisce l'autorità di dichiarare lo stato di crisi e stabilisce la catena di comando incaricata di gestire l'azienda in circostanze eccezionali. Sono previste misure di escalation rapide che consentano, una volta avuta consapevolezza della portata dell'incidente, di dichiarare lo stato di crisi in tempi brevi.

I processi per la gestione degli incidenti e per la dichiarazione e gestione dello stato di crisi sono formalizzati e strettamente integrati fra loro. Anche a tal fine, sono formalmente individuati i membri della struttura preposta alla gestione della crisi (ad es., Comitato di crisi), il responsabile della stessa struttura, la catena di comando, le modalità interne di comunicazione e le responsabilità attribuite alle funzioni aziendali interessate.

Il piano di continuità operativa stabilisce i tempi di ripristino dei processi critici[5], individua gli eventuali siti alternativi, prevede spazi e infrastrutture logistiche e di comunicazione adeguate per il personale coinvolto

[4] Ove il piano non sia articolato in piani settoriali, tali attività sono svolte dal responsabile del piano.
[5] Per i profili ICT il piano stabilisce, in particolare, il ripristino dell'operatività delle funzioni aziendali critiche, dei processi di supporto e delle risorse informatiche e tiene conto delle loro interdipendenze.

nella gestione della crisi, stabilisce le regole di conservazione delle copie dei documenti importanti (ad es., i contratti) in luoghi remoti rispetto ai documenti originali.

Il piano di continuità operativa dovrebbe anche considerare opzioni alternative per il caso in cui il ripristino non fosse fattibile nel breve periodo a causa di costi, rischi, fattori logistici o circostanze impreviste.

Con riferimento ai sistemi informativi centrali e periferici, il piano integra quello di *disaster recovery*[6]; quest'ultimo fornisce indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione, nonché sulle procedure per il ripristino presso gli eventuali siti alternativi.

La frequenza dei back-up è correlata alle dimensioni e alle funzioni[7] dell'operatore, tenendo conto della criticità dei dati; gli archivi di produzione dei processi critici sono duplicati almeno giornalmente. Sono assunte cautele per la corretta gestione del processo di conservazione delle copie elettroniche[8].

Il piano di continuità operativa definisce le modalità di comunicazione con la clientela, le controparti rilevanti, le autorità e i media.

Gli eventuali siti alternativi devono essere progettati e realizzati in modo da poter essere utilizzati, in caso di necessità, anche per periodi prolungati.

2.3.5 Verifiche

Gli operatori sottopongono periodicamente a verifica i propri piani di continuità operativa.

Le modalità di verifica delle misure di continuità dipendono dalla criticità dei processi e dai rischi individuati; di conseguenza sono ipotizzabili differenti frequenze e livelli di approfondimento delle verifiche. In alcuni casi può essere sufficiente la simulazione parziale dell'incidente o della catastrofe che può causare la crisi.

Con frequenza almeno annuale sono svolte verifiche complessive, basate su scenari il più possibile realistici, del ripristino della operatività dei processi critici in condizioni di crisi, riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano di continuità operativa. Le verifiche prevedono il coinvolgimento degli utenti finali, dei soggetti terzi di cui al paragrafo 2.3.7 e, laddove opportuno e possibile, delle controparti rilevanti.

Le verifiche annuali dei sistemi informativi prevedono l'attivazione dell'eventuale sito alternativo, il controllo dell'adeguata erogazione dei servizi in tale configurazione e in ogni caso prove di ripristino dei back-up di dati. Le prove sono preferibilmente realizzate con dati di produzione.

I risultati delle verifiche sono formalmente documentati, portati all'attenzione degli organi aziendali competenti e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di controllo (ad es. audit). In caso di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive.

2.3.6 Risorse umane

Il piano di continuità operativa individua il personale essenziale per assicurare la continuità dei processi critici e gli fornisce indicazioni dettagliate sulle attività da porre in essere in caso di crisi.

Le procedure di continuità operativa sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non impegnate nell'ordinaria attività dei processi cui si riferiscono.

Il personale coinvolto nel piano di continuità operativa è addestrato sulle misure da esso previste, accede alla lista di contatto e alla documentazione necessaria per operare in situazione di crisi, ha dimestichezza con gli

---

[6] In caso di outsourcing di componenti critiche del sistema informativo si applica quanto indicato al par. 2.3.7.

[7] Ad esempio, nel caso in cui svolga il ruolo di tramite per partecipanti indiretti.

[8] Per i processi non critici sono comunque adottati meccanismi per acquisire e gestire regolarmente copie di riserva dei dati e del software, al fine di assicurare l'integrità e la disponibilità delle informazioni. Per i siti alternativi off-line, in cui non siano presenti archivi di dati ovvero questi non siano allineati in tempo reale ai dati di produzione, sono definiti modalità e tempi per l'allineamento con i sistemi di produzione dopo il loro ripristino.

eventuali siti alternativi e con le apparecchiature in essi contenute, partecipa alle sessioni di verifica delle misure di continuità operativa.

Va valutata l'opportunità di frazionare l'attività connessa con i processi critici in più siti ovvero di organizzare il lavoro del personale su turni.

2.3.7 Ricorso a soggetti terzi per la prestazione di servizi ICT o per l'esternalizzazione, infrastrutture e controparti rilevanti

In caso di ricorso a soggetti terzi per la prestazione di servizi ICT o per l'esternalizzazione di funzioni aziendali connesse con lo svolgimento di processi critici, il piano di continuità operativa contiene le misure da attuare in caso di crisi con impatto rilevante sull'operatore o sul soggetto terzo.

In tali casi sono formalizzati contrattualmente i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal soggetto terzo, adeguati al conseguimento degli obiettivi aziendali e coerenti con le previsioni di questo allegato. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di Comitati utente, alle verifiche dei piani di continuità operativa dei soggetti terzi.

L'operatore acquisisce i piani del soggetto terzo o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate al suo interno. Il soggetto terzo comunica tempestivamente all'operatore il verificarsi di incidenti, al fine di consentire la pronta attivazione delle relative procedure di continuità.

Il piano di continuità operativa dell'operatore considera l'eventualità che le principali infrastrutture tecnologiche e/o finanziarie e le controparti rilevanti siano colpite da un evento catastrofico e stabilisce le misure per gestire i problemi conseguenti; la capacità di comunicare con gli eventuali siti alternativi di tali soggetti è verificata periodicamente.

Per i processi critici dell'operatore va valutata la possibilità di prevedere il ricorso, in casi di emergenza, a soggetti terzi alternativi. Nel caso in cui un soggetto terzo abbia impegnato le stesse risorse per fornire analoghi servizi ad altre aziende, in particolare se situate nella stessa zona, sono stabilite cautele contrattuali per evitare il rischio che, in caso di esigenze concomitanti di altre organizzazioni, le prestazioni degenerino o il servizio si renda di fatto indisponibile.

2.3.8 Controlli

Il piano di continuità operativa e il relativo processo di aggiornamento sono oggetto di regolare verifica da parte della funzione di revisione interna. L'*internal audit* prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, proponendo modifiche al piano sulla base delle mancanze riscontrate.

In tale ambito, particolare attenzione è posta all'analisi dei criteri di escalation. In caso di incidenti, la funzione di audit verifica la congruità dei tempi rilevati per la dichiarazione dello stato di crisi. La funzione di revisione interna è coinvolta anche nel controllo dei piani di continuità operativa dei soggetti terzi; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli. L'*internal audit* esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

Gli operatori considerano l'opportunità di sottoporre il piano di continuità operativa alla revisione da parte di competenti terze parti indipendenti.

2.3.9 Comunicazioni alla Banca d'Italia

In caso di incidenti con impatto sui propri processi critici e potenziali riflessi anche su altri operatori, l'operatore effettua una valutazione preliminare dell'entità degli eventuali impatti sistemici e segnala l'evento al Codise nei casi di particolare gravità, fornendo nel continuo gli aggiornamenti necessari per la gestione della crisi. Restano fermi gli obblighi di invio delle segnalazioni di incidenti alle autorità competenti secondo quanto previsto dalla normativa vigente.

Dopo il ripristino dei processi critici, l'operatore - anche nell'ambito della segnalazione di incidente prevista dalla normativa - fornisce con tempestività alla Banca d'Italia valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Gli operatori inviano alla Banca d'Italia un'informativa annuale sulle principali caratteristiche del piano di continuità operativa, sugli adeguamenti e integrazioni intervenuti in corso d'anno, sulle verifiche da parte dell'*internal audit*, sui principali incidenti e sulle criticità ricorrenti.

2.4 Aspettative ulteriori della funzione di sorveglianza della Banca d'Italia in proporzione al rischio

Gli operatori, avuto riguardo al profilo di rischio in funzione della dimensione, della complessità operativa, delle interdipendenze con altri soggetti finanziari, e delle specificità delle attività svolte e dei servizi offerti, si adoperano per raggiungere livelli di maturità progressivamente più elevati al fine di rafforzare la propria continuità operativa. A tal fine gli operatori fanno riferimento alle seguenti indicazioni.

Definizione del piano di continuità operativa e gestione delle crisi

(a) Scenari di rischio

Gli scenari di rischio rilevanti per la continuità operativa possono includere, oltre a quelli previsti nel paragrafo 2.1: eventi catastrofici con distruzioni fisiche su larga scala, a dimensione metropolitana o superiore, che investano infrastrutture essenziali dell'operatore e/o di terzi rilevanti; situazioni di crisi gravi anche non connesse con eventi con distruzioni materiali (ad es., pandemie, eventi chimico-biologici, attacchi informatici su larga scala).

(b) Siti alternativi

L'adozione di siti alternativi è una misura di particolare importanza per gli operatori, in relazione al loro profilo di rischio. I siti alternativi e il sito primario devono presentare un rischio di contemporanea indisponibilità trascurabile e/o essere situati a congrua distanza in modo da assicurare un elevato grado di indipendenza.

In generale, i siti alternativi sono ubicati all'esterno dell'area metropolitana nella quale sono presenti i siti primari; inoltre, essi utilizzano servizi (telecomunicazioni, energia, acqua, ecc.) distinti da quelli impiegati in produzione. Laddove ciò non avvenga è opportuna una valutazione rigorosa, supportata da pareri di parti terze qualificate (ad es., Protezione Civile, accademici, professionisti) e compiutamente documentata, che il rischio di indisponibilità contemporanea dei siti primari e alternativi è trascurabile.

I siti alternativi dei sistemi informativi sono configurati con capacità adeguata, all'occorrenza, a gestire volumi di attività attestati sui picchi massimi riscontrati nel corso dell'operatività ordinaria.

(c) Tempi di ripristino e percentuali di disponibilità

Gli operatori si adoperano affinché il tempo di ripristino non superi le quattro ore e il tempo di ripartenza non superi le due ore per i processi critici individuati di concerto con la Banca d'Italia in ragione dell'importanza per la piazza finanziaria italiana.

Se un evento catastrofico che colpisce un operatore determina un blocco di processi analoghi di altri operatori, questi ultimi si adoperano per ripristinare i propri processi critici entro due ore dalla ripartenza dell'operatore colpito in prima istanza.

Gli obiettivi di ripristino tengono conto di eventuali indicazioni fornite dalla Banca d'Italia e condivise nel Codise.

Con riferimento ai sistemi informativi, sono considerate adeguate le soluzioni basate su architetture tecnologiche che effettuino la duplicazione in linea dei dati operativi, in modo da eliminare o ridurre al minimo la perdita di informazioni. A tal fine gli operatori si adoperano affinché l'intervallo di tempo che intercorre fra il punto di ripristino e il momento dell'incidente (cd. RPO - *Recovery Point Objective*) sia pari o prossimo a zero.

È previsto, anche in caso di situazioni estreme, un ripristino quanto più possibile immediato dei processi critici, anche facendo ricorso a procedure a bassa integrazione nei processi aziendali, purché presidiate dal punto di vista della sicurezza (ad es., mediante l'utilizzo di PC off-line, contatti telefonici con controparti selezionate), in particolare per gestire le esigenze essenziali di liquidità.

(d) Risorse

Il piano di continuità operativa individua le risorse – umane, tecnologiche e logistiche – necessarie per l'operatività dei processi critici. Gli operatori si adoperano per garantire – con misure organizzative, mediante accordi con terzi, con la duplicazione del personale o con altri provvedimenti documentati – la presenza negli eventuali siti alternativi, all'occorrenza, del personale necessario per l'operatività dei processi critici. Va evitata la concentrazione, nello stesso luogo e allo stesso tempo, del personale chiave.

(e) Verifiche

Sono effettuate, con frequenza almeno annuale, verifiche accurate sui presidi delle misure di continuità operativa dei processi critici. Gli operatori si adoperano affinché venga assicurata la partecipazione attiva ai test e alle simulazioni di sistema organizzati o promossi dalle autorità, dai mercati e dalle principali infrastrutture finanziarie.

(f) Partecipazione al Codise

La Banca d'Italia si riserva di richiedere a specifici operatori la partecipazione stabile alle iniziative del Codise.