TITOLO IV

Capitolo 4

IL SISTEMA INFORMATIVO

TITOLO IV - Capitolo 4

IL SISTEMA INFORMATIVO

SEZIONE I

DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

Il sistema informativo (inclusivo delle risorse tecnologiche - hardware, software, dati, documenti elettronici, reti telematiche - e delle risorse umane dedicate alla loro amministrazione) rappresenta uno strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi degli intermediari, in considerazione della criticità dei processi aziendali che dipendono da esso. Infatti:

— dal punto di vista strategico, un sistema informativo sicuro ed efficiente, basato su un'architettura flessibile, resiliente e integrata a livello di gruppo consente di sfruttare le opportunità offerte dalla tecnologia per ampliare e migliorare i prodotti e i servizi per la clientela, accrescere la qualità dei processi di lavoro, favorire la dematerializzazione dei valori, ridurre i costi anche attraverso la virtualizzazione dei servizi bancari;

— nell'ottica della sana e prudente gestione, il sistema informativo consente al management di disporre di informazioni dettagliate, pertinenti e aggiornate per l'assunzione di decisioni consapevoli e tempestive e per la corretta attuazione del processo di gestione dei rischi (cfr. Capitolo 3);

— con riguardo al contenimento del rischio operativo, il regolare svolgimento dei processi interni e dei servizi forniti alla clientela, l'integrità, la riservatezza e la disponibilità delle informazioni trattate, fanno affidamento sulla funzionalità dei processi e dei controlli automatizzati;

— in tema di *compliance*, al sistema informativo è affidato il compito di registrare, conservare e rappresentare correttamente i fatti di gestione e gli eventi rilevanti per le finalità previste da norme di legge e da regolamenti interni ed esterni.

Le previsioni contenute nel presente Capitolo rappresentano requisiti di carattere generale per lo sviluppo e la gestione del sistema informativo da parte degli intermediari; le concrete misure da adottare tengono conto degli specifici obiettivi strategici e, secondo il principio di proporzionalità, della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati nonché del livello di automazione dei processi e servizi della banca.

A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e *best practices* definiti a livello internazionale in materia di governo, gestione, sicurezza e controllo del sistema informativo.

I requisiti di carattere generale sono integrati da requisiti organizzativi specifici da adottare in funzione dell'attività esercitata o di specifiche tipologie di rischio cui la banca è esposta. Particolare rilievo assumono i rischi assunti in relazione alla prestazione di servizi di pagamento (cfr. Sezione VII).

2. Fonti normative

La materia è regolata:

— dalle seguenti disposizioni del TUB:

- art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
- art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
- art. 67, comma 1, lett. d), il quale prevede che, al fine di esercitare la vigilanza consolidata, la Banca d'Italia impartisca alla capogruppo, con provvedimenti di carattere generale, disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;
- art. 146, comma 2 lett. b), che attribuisce alla Banca d'Italia il potere di emanare disposizioni aventi ad oggetto gli assetti organizzativi e di controllo relativi alle attività svolte nel sistema dei pagamenti;

e inoltre:

— dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;

— dal decreto del Ministro dell'Economia e delle finanze, Presidente del CICR del 5 agosto 2004 in materia, tra l'altro, di compiti e poteri degli organi sociali delle banche e dei gruppi bancari;

— dal decreto legislativo 27 gennaio 2010, n. 11, Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE, e successive modifiche e integrazioni;

dal regolamento della Commissione europea recante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (Regolamento delegato (UE) 2018/389 del 27 novembre 2017).

Vengono altresì in rilievo:

— la CRD IV;

- la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n.1093/2010, e abroga la direttiva 2007/64/CE (PSD2);
- dagli Orientamenti finali sulla sicurezza dei pagamenti via Internet, emanati dall'ABE il 19 dicembre 2014 ([2]);
- dagli Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2), emanati dall'ABE il 12 gennaio 2018 ([3])
- dagli Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2), emanati dall'ABE il 19 dicembre 2017.

Si è anche tenuto conto del documento *Principles for effective risk data aggregation and risk reporting*, pubblicato dal Comitato di Basilea per la vigilanza bancaria nel gennaio 2013 (4).

3. Definizioni

Ai fini della presente disciplina si definisce:

- "*accountability*": l'assegnazione della responsabilità di un'attività o processo aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili;
- "*autenticazione*": la procedura di verifica dell'identità di un utente da parte di un sistema o servizio;
- "*autorizzazione*": la procedura che verifica se un cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili;
-
- "*componente critica del sistema informativo*": il sistema o l'applicazione per i quali un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni operative importanti (cfr. Capitolo 3, par. 3) per l'intermediario, tra cui l'efficace espletamento dei compiti degli organi aziendali e delle funzioni di controllo; l'analisi dei rischi definisce le funzioni aziendali e le componenti del sistema informativo che presentano rischi rilevanti per la banca;
- "*credenziali*": le informazioni – generalmente riservate – utilizzate da un utente a fini di autenticazione ad un sistema o servizio. Sono inclusi nella definizione gli strumenti fisici

([2]) https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2
([3]) EBA/GL/2017/17.
(4) http://www.bis.org/publ/bcbs239.pdf.

che forniscono o memorizzano le informazioni (ad es., generatori di *password* non riutilizzabili, *smart card*) o qualcosa che l'utente ricorda (ad es., password) o rappresenta (ad es., caratteristiche biometriche);

— *"dati sensibili relativi ai pagamenti"*: dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate, ai sensi dell'articolo 1, comma 1, lett. q-*quater*, del d.lgs. 11/2010;

— "*incidente di sicurezza informatica*": ogni evento, o serie di eventi collegati, non pianificati dalla banca che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi);

— "*grave incidente di sicurezza informatica*": un incidente di sicurezza informatica da cui derivi o è probabile che derivi almeno una delle seguenti conseguenze:

  a. perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità;

  b. disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio;

  c. il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza;

  d. danni reputazionali, nel caso venga reso di pubblico dominio (ad esempio attraverso i media e gli organi di stampa).

— "*minimo privilegio* (*least privilege*)": il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati;

— "*no single point of failure*": il principio architetturale secondo il quale l'eventuale guasto di un singolo componente di un sistema non compromette il regolare funzionamento dell'intero sistema;

— "*operazioni critiche*": le operazioni relative a funzioni operative importanti effettuate in ambiente di produzione che, se errate o non effettuate, possono pregiudicare il regolare funzionamento di componenti critiche del sistema informativo (con riferimento a dati, a programmi o alla configurazione del sistema) nonché quelle che possono alterare, direttamente o indirettamente, i valori aziendali;

— "*procedura di contingency*": una procedura che, in caso di indisponibilità o grave malfunzionamento del sistema, prevede il ricorso in condizioni di emergenza a strumenti a bassa integrazione nei processi aziendali (ad es., ricorrendo ad attività manuali) al fine di completare un insieme limitato di operazioni di particolare criticità;

- "*procedura di fallback*": una procedura attivata in occasione di gravi problemi in caso di aggiornamento tecnologico o migrazione a nuove piattaforme, volta a fornire modalità alternative per lo svolgimento delle funzioni applicative non funzionanti;
- "*rischio informatico* (*o ICT*)": il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (*Information and Communication Technology* – ICT). Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici;
- "*rischio informatico residuo*": il rischio informatico a cui l'intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi;
- "*risorsa informatica* (*o ICT*)": un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dall'intermediario;
- "*segregazione dei compiti* (*segregation of duties*)": il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;
- "*utente responsabile*": la figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica;
- "*verificabilità*": la garanzia di poter ricostruire, all'occorrenza e anche a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati.

4. Destinatari della disciplina

Le presenti disposizioni si applicano:

- alle banche italiane e alle succursali di banche extracomunitarie, ad eccezione di quelle aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive (5); queste ultime si attengono esclusivamente a quanto previsto dalla Sezione VII, par. 1, con riferimento alla prestazione di servizi di pagamento;
- alle capogruppo di gruppi bancari;
- alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 3.

(5) Alle banche che prestano attività e servizi di investimento si applicano anche le disposizioni contenute nel Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, come successivamente modificato e integrato, in materia di organizzazione e procedure degli intermediari che prestano servizi di investimento o di gestione collettiva del risparmio.

SEZIONE II

GOVERNO E ORGANIZZAZIONE DEL SISTEMA INFORMATIVO

1. Premessa

Nell'ambito della generale disciplina dell'organizzazione e dei controlli interni, sono attribuiti agli organi e funzioni aziendali ruoli e responsabilità, relativi allo sviluppo e alla gestione del sistema informativo, nel rispetto del principio della separazione delle funzioni di controllo da quelle di supervisione e gestione.

2. Compiti dell'organo con funzione di supervisione strategica

L'organo con funzione di supervisione strategica assume la generale responsabilità di indirizzo e controllo del sistema informativo, nell'ottica di un ottimale impiego delle risorse tecnologiche a sostegno delle strategie aziendali (*ICT governance*). In tale ambito esso:

— approva le strategie di sviluppo del sistema informativo, in considerazione dell'evoluzione del settore di riferimento e in coerenza con l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale; in tale contesto approva il modello di riferimento per l'architettura del sistema informativo;

— approva la *policy* di sicurezza informatica (1);

— approva le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni (cfr. Sezione VI);

— promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda;

— è informato con cadenza almeno annuale circa l'adeguatezza dei servizi erogati e il supporto di tali servizi all'evoluzione dell'operatività aziendale, in rapporto ai costi sostenuti; è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo.

Con specifico riguardo all'esercizio della responsabilità di supervisione della analisi del rischio informatico (cfr. Sezione III), lo stesso organo:

— approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della funzione ICT e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici);

(1) Nel caso di *full outsourcing* del sistema informativo l'organo di supervisione strategica, qualora non abbia le necessarie competenze al proprio interno, potrà avvalersi di risorse esterne indipendenti dal fornitore di servizi. Inoltre, nella definizione dei documenti richiesti (cfr. Allegato A), si può fare riferimento ad analoga documentazione prodotta dal fornitore.

— approva la propensione al rischio informatico, avuto riguardo ai servizi interni e a quelli offerti alla clientela, in conformità con gli obiettivi di rischio e il quadro di riferimento per la determinazione della propensione al rischio definiti a livello aziendale (cfr. Capitolo 3, Allegato C);

— è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio.

Nell'Allegato A, sono riportati i documenti che l'organo con funzione di supervisione strategica approva nell'ambito del suo ruolo e responsabilità nella materia.

3. Compiti dell'organo con funzione di gestione

L'organo con funzione di gestione ha il compito di assicurare la completezza, l'adeguatezza, la funzionalità (in termini di efficacia ed efficienza) e l'affidabilità del sistema informativo. In particolare, tale organo:

— definisce la struttura organizzativa della funzione ICT (ove presente) (2) assicurandone nel tempo la rispondenza alle strategie e ai modelli architetturali definiti dall'organo con funzione di supervisione strategica; garantisce il corretto dimensionamento quali-quantitativo delle risorse umane;

— definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico, perseguendo un opportuno livello di raccordo con la funzione di *risk management* per i processi di stima del rischio operativo;

— tranne che nel caso di *full outsourcing,* approva il disegno dei processi di gestione del sistema informativo, garantendo l'efficacia ed efficienza dell'impianto nonché la complessiva completezza e coerenza, con particolare riguardo ad una funzionale assegnazione di compiti e responsabilità, alla robustezza dei controlli, alla validità del supporto metodologico e procedurale;

— approva gli standard di *data governance*, le procedure di gestione dei cambiamenti e degli incidenti (ove del caso, in raccordo con le procedure del fornitore di servizi) e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di *business* nonché con le strategie aziendali;

— valuta almeno annualmente le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi / benefici o utilizzando sistemi integrati di misurazione delle prestazioni (3), assumendo gli opportuni interventi e iniziative di miglioramento;

(2) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata del gruppo, il compito di definizione della funzione ICT può essere demandato all'organo con funzione di gestione di tale società, previa individuazione di opportuni canali informativi verso gli organi aziendali della capogruppo.

(3) I sistemi integrati di misurazione e *reporting* delle prestazioni sono procedure automatizzate, di norma basate su metodologie (ad es., *balanced scorecards*) volte a tracciare un profilo integrato del complessivo andamento dell'azienda o di una specifica funzione aziendale, attraverso il ricorso ad indicatori di prestazione (*KPI – key performance indicators*) e valori di riferimento (*benchmark*) opportunamente individuati. In caso di *outsourcing* è opportuno definire nel contratto un insieme di *report* minimi, utili anche a verificare il rispetto delle SLA (*Service level agreement*).

- approva almeno annualmente la valutazione del rischio delle componenti critiche nonché la relazione sull'adeguatezza e costi dei servizi ICT, informando a tale riguardo l'organo con funzione di supervisione strategica; in tale ambito, riscontra la complessiva situazione del rischio informatico in rapporto alla propensione al rischio definita, disponendo allo scopo di idonei flussi informativi concernenti, come minimo, il livello di rischio residuo per le diverse risorse informatiche, lo stato di implementazione dei presidi di attenuazione del rischio (cfr. Sezione III), l'evoluzione delle minacce connesse con l'utilizzo di ICT nonché gli incidenti registratisi nel periodo di riferimento;
- monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive;
- assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica (cfr. Sezione IV) e fornisce informazioni all'organo con funzione di supervisione strategica in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti.

In relazione alla responsabilità e ai compiti assegnati, l'organo con funzione di gestione è dotato di competenze tecnico – manageriali, tenuto conto della dimensione, complessità e articolazione organizzativa dell'intermediario nonché delle strategie di *sourcing.*

Nell'Allegato A sono riportati le procedure, gli standard e i piani soggetti all'approvazione dell'organo con funzione di gestione.

4. Organizzazione della funzione ICT

L'articolazione organizzativa della funzione ICT dipende da fattori quali la complessità della struttura societaria, la dimensione, i settori di attività, le strategie di *business* e gestionali. Essa si ispira a criteri di funzionalità, efficienza e sicurezza, definendo chiaramente compiti e responsabilità e contemplando in particolare:

- linee di riporto dirette a livello dell'organo con funzione di gestione (4) a garanzia dell'unitarietà della visione gestionale e del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti il sistema informativo; eventuali unità di sviluppo decentrato sotto il controllo delle linee di *business* sono comunque inquadrate nel più generale disegno architetturale e agiscono nell'ambito di regole definite a livello aziendale;
- le responsabilità e gli assetti connessi con la pianificazione e il controllo del portafoglio dei progetti informatici, con il governo dell'evoluzione dell'architettura e dell'innovazione tecnologica nonché con le attività di gestione del sistema informativo (5);
- la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*, con particolare riguardo alle attività di individuazione e pianificazione delle iniziative

(4) Nel caso di gruppo bancario che abbia accentrato la funzione ICT in una società controllata, è possibile individuare all'interno di questa l'organo responsabile di tale funzione per l'intero gruppo, purché siano stabiliti canali informativi diretti tra esso e l'organo con funzione di gestione della capogruppo; in tale opzione, l'organo con funzione di gestione della capogruppo assume la responsabilità di seguire la pianificazione delle iniziative ICT, garantendone la rispondenza alle esigenze e alle strategie del gruppo.

(5) Nel caso di *full outsourcing* della funzione ICT, al "referente per l'attività esternalizzata" (cfr. Capitolo 3, Sezione IV, par. 1) è assegnata la responsabilità di seguire la pianificazione dei progetti informatici; la stessa figura garantisce, in collaborazione con il fornitore di servizi, la realizzazione degli opportuni meccanismi di raccordo con le linee di *business*.

informatiche (regolare rilevazione delle esigenze di servizi informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione del sistema informativo).

5. La sicurezza informatica

La funzione di sicurezza informatica è deputata allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT. In particolare:

— segue la redazione e l'aggiornamento delle *policy* di sicurezza e delle istruzioni operative;

— assicura la coerenza dei presidi di sicurezza con le *policy* approvate;

— partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei *data center*;

— partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico (cfr. Sezione III);

— assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche (cfr. Sezione IV, par. 3);

— segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo o modificato (cfr. Sezione IV, par. 5).

Nelle realtà più complesse, l'indipendenza di giudizio rispetto alle funzioni operative è assicurata da un'adeguata collocazione organizzativa.

6. Il controllo del rischio informatico e la *compliance* ICT

Nell'ambito del sistema dei controlli interni sono chiaramente assegnate responsabilità in merito allo svolgimento dei seguenti compiti di controllo di secondo livello:

— il controllo dei rischi, basato su flussi informativi continui in merito all'evoluzione del rischio informatico e sul monitoraggio dell'efficacia delle misure di protezione delle risorse ICT. La gestione del complessivo rischio informatico si raccorda con il processo di analisi sulle singole risorse ICT (cfr. Sezione III). Le valutazioni svolte sono documentate e riviste in rapporto ai risultati del monitoraggio e comunque almeno una volta l'anno.

  Con riferimento alle banche con un modello interno validato sul rischio operativo, i dati sulle perdite operative in ambito ICT sono integrati con i dati e gli scenari relativi alle altre funzioni aziendali, e ne sono presidiati la qualità e completezza;

— il rispetto dei regolamenti interni e delle normative esterne in tema di ICT (ICT *compliance*) garantendo, tra l'altro:

  - l'assistenza su aspetti tecnici in caso di questioni legali relative al trattamento dei dati personali;
  - la coerenza degli assetti organizzativi alle normative esterne, per le parti relative al sistema informativo;

- l'analisi di conformità dei contratti di *outsourcing* e con fornitori (inclusi i contratti infra-gruppo).

7. Compiti della funzione di revisione interna

L'*internal audit* dispone - al suo interno o mediante il ricorso a risorse esterne (6) - delle competenze specialistiche necessarie per assolvere ai propri compiti di *assurance* attinenti al sistema informativo aziendale (ICT *audit*).

La pianificazione degli interventi ispettivi assicura nel tempo un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, incluse le eventuali componenti esternalizzate (7). A prescindere dalla forma adottata per gli accertamenti (ad es., *audit* mirati ovvero verifiche sulle applicazioni e componenti del sistema informativo nell'ambito di ispezioni su strutture organizzative o processi produttivi), la frequenza e il contenuto dei controlli tengono conto del complessivo profilo di rischio del processo o sistema oggetto di verifica, con particolare riguardo ai rischi di sicurezza. L'*internal audit* è in grado di fornire valutazioni sui principali rischi tecnologici identificabili e sulla complessiva gestione del rischio informatico dell'intermediario.

(6) Anche in caso di ricorso all'esterno, le risorse impegnate nell'*audit* mantengono l'indipendenza rispetto alle unità assoggettate al controllo.

(7) Tenuto conto del principio di proporzionalità, per le verifiche su componenti o servizi ICT esternalizzati, la funzione di *audit* dell'intermediario potrà scegliere, sotto la sua responsabilità, di fare affidamento sull'*internal audit* del fornitore di servizi, previa valutazione della sua professionalità e indipendenza.

SEZIONE III

L'ANALISI DEL RISCHIO INFORMATICO

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario.

L'attività è svolta nell'ambito delle iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo. Il processo è ripetuto con periodicità adeguata alla tipologia delle risorse ICT e dei rischi (1), nonché, tempestivamente, al verificarsi di situazioni che possono influenzare il complessivo livello di rischio informatico (2).

Il processo di analisi è svolto con il concorso dell'utente responsabile (3), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:

- la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; questa fase prende l'avvio con la classificazione delle risorse ICT (5) in termini di rischio informatico (6) e prevede l'identificazione degli scenari di rischio rilevanti e delle minacce che insidiano la sicurezza dei processi e delle risorse;
- il trattamento del rischio, volto a individuare le misure di attenuazione – di tipo tecnico, organizzativo, procedurale o strategico – idonee a contenere il rischio potenziale, sulla base delle risultanze della fase precedente.

L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (7). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (8), definite con il

(1) Per i sistemi non critici il processo è ripetuto almeno ogni tre anni; per le componenti critiche del sistema informativo cui è assegnato l'indicatore di criticità più elevato, il processo di analisi del rischio è effettuato con cadenza annuale. La Banca Centrale Europea e la Banca d'Italia possono richiedere frequenze maggiori.

(2) Tra le situazioni suscettibili di modificare gli scenari di rischio e il livello di rischio informatico valutato – e che quindi richiedono la revisione dell'analisi del rischio – sono incluse: modifiche al contesto operativo esistente, il verificarsi di gravi incidenti, la rilevazione di carenze nei controlli, la diffusione di notizie su nuove vulnerabilità o minacce.

(3) Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. In caso di esternalizzazione del sistema, il referente per l'attività esternalizzata (cfr. Capitolo 3, Sezione IV, par. 1) partecipa, in qualità di utente responsabile, all'analisi del rischio svolta dal fornitore di servizi, anche tramite "comitati utente"; nel caso di *full outsourcing* presso una società strumentale del gruppo di appartenenza, l'utente responsabile è collocato all'esterno della funzione ICT (ad es., presso la capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato).

(5) La classificazione delle informazioni gestite mediante strumenti ICT è opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento.

(6) Ad esempio, con riferimento alla sicurezza informatica, va assegnato un indicatore di criticità in relazione al potenziale impatto di eventuali violazioni dei livelli di riservatezza, integrità, disponibilità richiesti dall'utente responsabile e alla probabilità di accadimento delle minacce che potrebbero causare tali violazioni.

(7) Nel documento approvato dall'utente responsabile, il rischio residuo è chiaramente espresso, perlomeno in termini qualitativi e con una descrizione non tecnica degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

(8) Ad esempio, si potrebbe ritenere di non abilitare funzioni o operazioni troppo rischiose (*risk avoidance*), ovvero di acquisire una polizza assicurativa (*risk transfer*).

coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

Per le procedure in esercizio (9) per le quali siano stati individuati successivamente eventuali presidi in aggiunta a quelli già in essere, è adottato un piano di implementazione specifico. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione, sono documentati e sottoposti all'accettazione formale dell'utente responsabile. In ogni caso, l'aggiornamento delle misure di sicurezza che riguardano componenti critiche è effettuato senza indebiti ritardi.

I risultati del processo (livelli di classificazione, rischi potenziali e residui, lista delle minacce considerate, elenco dei presidi individuati), ogni loro aggiornamento successivo, le assunzioni operate e le decisioni assunte, sono documentati e portati a conoscenza dell'organo con funzione di gestione.

(9) In sede di valutazione dei rischi su componenti del sistema informativo e applicazioni già in essere, la banca tiene conto dei dati disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato (cfr. Sezione IV, par. 6).

SEZIONE IV

LA GESTIONE DELLA SICUREZZA INFORMATICA

1. Premessa

La gestione della sicurezza informatica comprende i processi e le misure volti, in raccordo con la generale azione aziendale per preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability*, appropriata e coerente lungo l'intero ciclo di vita.

Obiettivo di tale processo è anche di contribuire alla conformità del sistema informativo alle norme di legge e ai regolamenti interni ed esterni.

La struttura dei processi e l'intensità dei presidi da porre in atto dipende dalle risultanze del processo di analisi dei rischi (cfr. Sezione III).

2. *Policy* di sicurezza

La *policy* di sicurezza informatica è approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale e alle terze parti coinvolte nella gestione di informazioni e componenti del sistema informativo. Essa riporta:

- gli obiettivi del processo di gestione della sicurezza informatica in linea con la propensione al rischio informatico definito a livello aziendale (cfr. Sezione II, par. 2); tali obiettivi sono espressi in termini di esigenze di protezione e di controllo del rischio tecnologico;
- i principi generali di sicurezza sull'utilizzo e la gestione del sistema informativo da parte dei diversi profili aziendali;
- i ruoli e le responsabilità connessi alla funzione di sicurezza informatica, nonché le linee di riporto gerarchico per l'attuazione delle misure di sicurezza e la gestione dei rischi relativi;
- i ruoli e le responsabilità connessi all'aggiornamento e alla verifica delle *policy*;
- il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione;
- le linee di indirizzo per le attività di comunicazione, formazione e sensibilizzazione delle diverse classi di utenti, che includono almeno: (i) per tutti i dipendenti, un programma di formazione con cadenza annuale o, se necessario, maggiore per assicurare il rispetto di della policy e delle procedure di sicurezza della banca nell'adempimento dei compiti e delle responsabilità assegnate; (ii) per i soggetti incaricati di funzioni critiche, una formazione mirata con cadenza annuale o, se necessario, maggiore sulla sicurezza delle informazioni; (iii) programmi periodici di sensibilizzazione sulla sicurezza al fine di accrescere il grado di consapevolezza dei dipendenti sui rischi relativi alla sicurezza informatica e incentivare la segnalazione di attività insolite o eventuali incidenti;

— un richiamo alle norme interne che disciplinano le conseguenze di violazioni rilevate della *policy* da parte del personale;

— un richiamo alle norme di legge e alle altre normative esterne applicabili inerenti alla sicurezza di informazioni e risorse ICT, incluse le norme riportate nella presente Sezione.

La *policy* di sicurezza può fare riferimento a documenti di maggiore dettaglio, ad es. linee guida o manuali operativi in tema di configurazioni e procedure di sicurezza per particolari componenti e applicazioni; *policy* dedicata per i servizi di pagamento; norme per il corretto utilizzo di applicazioni aziendali trasversali, quali la posta elettronica e la navigazione internet.

La regolare revisione della *policy* di sicurezza tiene conto dell'evoluzione del campo di attività, dei prodotti forniti, delle tecnologie, delle modalità di approvvigionamento dei servizi e dei rischi fronteggiati dall'intermediario (cfr. Sezione III).

3. La sicurezza delle informazioni e delle risorse ICT

La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di sicurezza a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza).

Le misure di sicurezza sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità"); esse comprendono:

— i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es., barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);

— la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative (principio del *need to know)*; i diritti di accesso sono accordati, di norma, secondo l'approccio dell'accesso basato sulle funzioni (c.d. *role-based access control*), previa formale autorizzazione. L'autorizzazione è rilasciata a personale adeguatamente addestrato e soggetto a monitoraggio, mediante ricorso ad opportuni profili abilitativi; l'elenco degli utenti abilitati è sottoposto a verifica con periodicità definita. La gestione di prodotti, strumenti e procedure relativi ai processi di controllo degli accessi garantisce la protezione di questi processi da tentativi di compromissione o elusione, in particolare con riferimento alla sottoscrizione, alla consegna, alla revoca e al ritiro di questi prodotti, strumenti e procedure;

— la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi; in particolare sono garantiti l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione (1), l'osservanza degli standard definiti all'interno nonché delle normative applicabili, ad es. in materia di composizione e

(1) La procedura di generazione e di gestione dei fattori delle credenziali di autenticazione (ad es., password, *smart card, token*) garantisce che essi siano unici e nella disponibilità esclusiva del legittimo utente assegnatario, fatta salva la possibilità di definire procedure sicure per permettere all'intermediario di accedere a dati aziendali in caso di necessità, in assenza degli utenti abilitati.

gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

— la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es., sistemi e utenti interni, applicazioni *core,* sistemi e utenti esterni); l'accesso a sistemi e servizi critici tramite canali pubblici (ad es., nel caso dell'*e-banking* tramite internet o altri canali digitali) sono presidiati in modo da soddisfare rigorosi requisiti di sicurezza e fornire un livello di protezione conforme ai rischi da fronteggiare; con riferimento ai servizi di pagamento tramite internet si applicano gli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" emanati dall'ABE, secondo quanto specificato nella Sezione VII;

— l'adozione di metodologie e tecniche per lo sviluppo sicuro del software quale possibile presidio di difesa per componenti valutate nell'analisi del rischio informatico a un livello di rischio potenziale elevato;

— con riferimento alle componenti critiche del sistema informativo, l'adozione di procedure per l'aggiornamento *software* (inclusa l'applicazione delle *patch* critiche per la sicurezza) e di meccanismi di controllo dell'integrità del *software*, del *firmware* e delle informazioni;

— la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli *software* tra di essi (par. 5), al fine di evitare – di norma – l'accesso a dati riservati e componenti critiche da parte del personale addetto allo sviluppo (2); l'ambiente di produzione è sottoposto a misure più restrittive di controllo degli accessi e delle modifiche;

— i criteri per la selezione e la gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti privilegiati) con particolare riguardo alla valutazione delle competenze e dell'affidabilità del personale, alla stipula di specifici impegni di riservatezza nonché alla gestione nel continuo delle mansioni assegnate (ad es., per mezzo di verifiche periodiche degli elenchi del personale abilitato e di misure di *job rotation*);

— le procedure per lo svolgimento delle operazioni critiche, garantendo il rispetto dei principi del minimo privilegio e della segregazione dei compiti (ad es., specifiche procedure di abilitazione e di autenticazione, controlli di tipo *four eyes* (3), o di verifica giornaliera *ex post*). L'accesso a componenti critiche del sistema informativo da parte di utenti privilegiati o amministratori di sistema è effettuato attraverso procedure di autenticazione rafforzate, come l'autenticazione a più fattori ("autenticazione forte") (4);

— il monitoraggio, anche attraverso l'analisi di log e tracce di *audit*, di accessi, operazioni e altri eventi al fine di prevenire e gestire gli incidenti di sicurezza informatica; le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;

(2) Tale accesso può essere concesso agli sviluppatori in casi specificamente disciplinati, in via temporanea e previa autorizzazione dell'utente responsabile.

(3) Si fa riferimento a controlli applicativi che richiedono l'inserimento di una stessa transazione da parte di due diversi utenti per procedere alla sua esecuzione.

(4) L'accesso amministrativo da remoto a componenti critiche dei sistemi ICT è sempre effettuato attraverso procedure di autenticazione forte ed è concesso esclusivamente sulla base di specifiche esigenze.

- il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza, con particolare riguardo a: i) i fattori interni ed esterni importanti, comprese le funzioni di gestione del business e dell'ICT aziendali; ii) le transazioni, al fine di individuare eventuali abusi negli accessi da parte dei fornitori o di altri soggetti; iii) le potenziali minacce interne ed esterne;
- le scansioni delle vulnerabilità ("*vulnerability scan*") e le prove di penetrazione ("*penetration test*") adeguate al profilo di rischio informatico individuato dall'analisi di rischio;
- le regole di tracciabilità degli accessi e delle operazioni effettuate, finalizzate a individuare le attività anomale e a svolgere le relative indagini, nonché alla verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora (5), contesto operativo e altre caratteristiche salienti della transazione. Le registrazioni sono conservate in archivi non modificabili o le cui modifiche sono puntualmente registrate per un periodo commisurato al livello di criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche, documentato negli inventari aziendali (6).

4. La sicurezza delle applicazioni sviluppate dalle unità operative e di controllo

Lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo è sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni sviluppate dalla funzione ICT.

Un periodico monitoraggio censisce le applicazioni sviluppate con strumenti di informatica d'utente e ne verifica la rispondenza alla *policy* di sicurezza, in particolare se utilizzate in attività rilevanti quali la predisposizione dei dati di bilancio, del *risk management*, della finanza e del *reporting* direzionale, al fine di contenere il rischio operativo (7).

5. La gestione dei cambiamenti

La procedura di gestione dei cambiamenti delle applicazioni e risorse ICT è formalmente definita e garantisce il controllo su modifiche, sostituzioni o adeguamenti tecnologici, in particolare nell'ambiente di produzione. Il processo si svolge sotto la responsabilità di una figura o struttura aziendale con elevato grado di indipendenza rispetto alla funzione di sviluppo e prevede, in modo proporzionato alla complessità e al profilo di rischio tecnologico dell'intermediario:

(5) Ai fini della possibilità di una corretta e agevole ricostruzione di eventi e operazioni che coinvolgono più sistemi, inclusi eventualmente sistemi esterni, è opportuno che l'intermediario si doti di un sistema unificato di riferimento temporale, ad es. basato sul protocollo standard NTP e sincronizzato con un segnale orario di riferimento ufficiale.

(6) Restano fermi gli obblighi di conservazione di dati e documenti previsti dalla normativa appplicabile.

(7) Tale censimento è anche utile a verificare il grado di copertura delle esigenze garantito dalle procedure messe a disposizione dalla funzione ICT.

- la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio ICT (*hardware*, *software*, dati, procedure), incluse le interconnessioni con sistemi esterni (8);
- la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;
- l'autorizzazione formale di ogni cambiamento in ambiente di produzione (9); tale procedura comprende l'accettazione, nei casi critici individuati nell'analisi dei rischi, nel nuovo rischio residuo;
- la pianificazione, il coordinamento e la documentazione degli interventi di modifica, prevedendo attività di collaudo e test di sicurezza, in un ambiente deputato e distinto da quello di produzione;
- il ricorso a un idoneo sistema di gestione della configurazione di sistema (hardware, software, procedure di gestione e utilizzo, modalità di interconnessione), per il controllo dell'implementazione dei cambiamenti, inclusa la possibilità di ripristino della situazione *ex ante*.

Le modifiche in caso di emergenza possono essere gestite con presidi non pienamente conformi alle *policy* ordinarie ma comunque adeguati alla particolare situazione. Tali modifiche sono comunque sottoposte a tracciamento e notificate *ex post* all'utente responsabile.

Le iniziative di ampio impatto sul sistema informativo (ad es., modifiche rilevanti sulle componenti critiche, adeguamenti in conseguenza di fusioni o scissioni, migrazione ad altre piattaforme informatiche) – che si inseriscono di norma in piani strategici all'attenzione dell'organo con funzione di supervisione strategica – sono preventivamente comunicate alla Banca centrale europea o alla Banca d'Italia e prevedono, in aggiunta a quanto sopra specificato, idonee misure, tecniche, organizzative e procedurali, volte a garantire un avvio in esercizio controllato e con limitati impatti sui servizi forniti alla clientela (ad es., implementazione per stadi successivi, periodi di esercizio in parallelo con la precedente procedura, procedure di *fallback* e *contingency*). Flussi informativi verso i vari livelli manageriali e gli organi aziendali consentono il monitoraggio dell'avanzamento del progetto.

6. La gestione degli incidenti di sicurezza informatica

La gestione degli incidenti di sicurezza informatica segue procedure formalmente definite, con l'obiettivo di minimizzarne l'impatto e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti. Le funzioni a cui comunicare l'incidente sono individuate secondo un'opportuna procedura di *escalation*; i casi più gravi che comportino rischi di interruzione della continuità operativa sono segnalati alla struttura preposta a dichiarare lo stato di crisi (cfr. Capitolo 5).

(8) L'inventario aggiornato del sistema e delle risorse ICT è funzionale anche alle attività di analisi del rischio informatico (cfr. Sezione III).

(9) Il livello autorizzativo è adeguato all'entità dei rischi emersi nell'analisi.

A seguito dell'analisi degli incidenti di sicurezza informatica e dei relativi rilievi delle funzioni di *audit* e della *compliance* sono definite e monitorate le azioni correttive.

In ogni caso, le informazioni salienti dell'evento e i passi seguiti nella gestione dello stesso sono documentati.

Il processo si raccorda con il monitoraggio di sistemi, accessi e operazioni (cfr. par. 3) nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione e la definizione di indicatori di preallerta che consentano l'individuazione precoce degli incidenti (10).

Le procedure definite per gravi incidenti di sicurezza informatica includono la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti, anche in caso di fuoriuscite di informazioni.

I gravi incidenti di sicurezza informatica sono notificati tempestivamente alla Banca d'Italia, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela, nonché degli altri dati e informazioni previsti dalle istruzioni emanate dalla Banca d'Italia (11).

7. La disponibilità delle informazioni e delle risorse ICT

La disponibilità dell'accesso a dati e dei servizi telematici è garantita agli utenti autorizzati in orari e con modalità conformi alle esigenze (12). A tal fine, i processi interessati (definizione dei modelli architetturali, sviluppo di applicazioni e infrastrutture, gestione dei problemi tecnici, monitoraggio e pianificazione della capacità elaborativa e trasmissiva, gestione dei fornitori) tengono conto delle seguenti indicazioni:

— con riguardo alle applicazioni di maggiore criticità e ai servizi ICT rivolti alla clientela sono formalmente definiti i livelli di servizio che l'intermediario si impegna ad osservare; le prestazioni delle componenti critiche rispetto a tali livelli sono regolarmente monitorate e formano oggetto di sintetici rapporti disponibili periodicamente a tutte le parti interessate; è assicurata la congruità tra i livelli di servizio definiti per le componenti tra loro dipendenti;

— in relazione alle esigenze di disponibilità delle singole applicazioni, sono definite procedure di *backup* (di dati, software e configurazione) e di ripristino su sistemi alternativi, in precedenza individuati;

— le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del *no single point of failure*) volte a garantire l'alta disponibilità

(10) Nel caso delle banche AMA il processo è integrato con la rilevazione delle perdite operative.

(11) Le istruzioni specificano i criteri per l'identificazione degli incidenti "gravi", le modalità e tempi della segnalazione, tenuto conto degli "Orientamenti in materia di segnalazione dei gravi incidenti ai sensi della direttiva (UE) 2015/2366 (PSD2)" emanati dall'ABE il 19 dicembre 2017 (EBA/GL/2017/10) (cfr. Sezione VII). Le istruzioni sono pubblicate sul sito *internet* della Banca d'Italia.

(12) Si tiene conto del profilo di utilizzo (noto o stimato) nell'arco del calendario e per l'orario di operatività, con particolare attenzione a eventuali picchi elaborativi.

delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di *disaster recovery;*

- in funzione dei profili di rischio delle comunicazioni, delle applicazioni e dei servizi acceduti, i collegamenti telematici interni alla banca o al gruppo sono opportunamente ridondati; in relazione al rischio di incidenti di sicurezza informatica che possono determinare l'interruzione dei servizi (ad es., mediante attacchi di tipo *denial of service o distributed denial of service*), oltre a soluzioni specifiche per l'individuazione e il blocco del traffico malevolo, la banca valuta l'opportunità di sfruttare procedure e strumenti per l'allocazione dinamica di capacità trasmissiva ed elaborativa;
- la gestione del sistema informativo è opportunamente automatizzata e si avvale, per quanto possibile, di procedure standardizzate; le operazioni di manutenzione ordinaria e straordinaria sono pianificate e comunicate con congruo anticipo agli utenti interessati;
- le informazioni raccolte attraverso il processo di monitoraggio delle risorse ICT alimentano il regolare processo di *capacity planning* (13) e sono utilizzate nella progettazione dell'evoluzione del sistema informativo.

(13) Si intende per *capacity planning* il processo di gestione dell'ICT volto a stimare la quantità di risorse informatiche necessarie a fronteggiare le esigenze delle applicazioni aziendali nell'arco di un determinato periodo futuro.

SEZIONE V

IL SISTEMA DI GESTIONE DEI DATI

Il sistema di registrazione e *reporting* dei dati è deputato a tracciare tempestivamente tutte le operazioni aziendali e i fatti di gestione al fine di fornire informazioni complete e aggiornate sulla attività aziendali e sull'evoluzione dei rischi. Esso assicura nel continuo l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate; inoltre, garantisce l'*accountability* e l'agevole verificabilità (ad es., da parte delle funzioni di controllo) delle operazioni registrate.

In particolare, il sistema di gestione dei dati soddisfa i seguenti requisiti:

— la registrazione dei fatti aziendali è completa, corretta e tempestiva, al fine di consentire la ricostruzione dell'attività svolta (1);

— è definito uno standard aziendale di *data governance*, che individua ruoli e responsabilità delle funzioni coinvolte nell'utilizzo e nel trattamento, a fini operativi e gestionali delle informazioni aziendali (2); in considerazione della loro rilevanza nel sistema informativo, sono definite le misure atte a garantire e a misurare la qualità (3), ad es. attraverso *key quality indicator* riportati periodicamente agli utenti di *business*, alle funzioni di controllo e all'organo con funzione di gestione;

— la identificazione, la misurazione o la valutazione, il monitoraggio, la prevenzione o l'attenuazione dei rischi connessi con la qualità dei dati fa parte del processo di gestione dei rischi (cfr. Capitolo 3); in caso di acquisizione o incorporazione di soggetti esterni, la *due diligence* comprende la valutazione dell'impatto dell'operazione sulle procedure di gestione e aggregazione dei dati; l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non compromette la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, il sistema di gruppo assicura l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo;

— nel caso di ricorso a un *data warehouse* aziendale a fini di analisi e *reporting*, le procedure di estrazione dei dati, di trasformazione, controllo e caricamento negli archivi accentrati – così come le funzioni di sfruttamento dei dati – sono dettagliatamente documentate, al fine di consentire la verifica sulla qualità dei dati;

— le procedure di gestione e aggregazione dei dati sono documentate, con specifica previsione delle circostanze in cui è ammessa l'immissione o la rettifica manuale di dati aziendali,

(1) I controlli sulle registrazioni contabili verificano, tra l'altro, le procedure per l'individuazione e sistemazione delle divergenze tra saldi dei sottosistemi sezionali e quelli della contabilità generale, i processi di quadratura tra i documenti di *front-office* e le registrazioni giornaliere; la conferma periodica dei rapporti con controparti e clienti. Le verifiche riguardano anche l'allineamento tra i dati utilizzati per la gestione dei rischi e per la rendicontazione finanziaria.

(2) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capito I.5) individuano per i dati rilevanti (informazione al mercato, segnalazioni all'Organo di Vigilanza, valutazione dei rischi, ecc.) una o più figure aziendali responsabili di assicurare lo svolgimento dei controlli previsti e della validazione della qualità dei dati (c.d. "*data owner*"). Le procedure di aggregazione dei dati a fini di valutazione dei rischi aziendali sono sottoposte a validazione indipendente (ad es., da parte dell'*internal audit)*.

(3) La qualità dei dati è valutata, in termini di completezza (registrazione di tutti gli eventi, operazioni e informazioni con i pertinenti attributi necessari per le elaborazioni), di accuratezza (assenza di distorsione nei processi di registrazione, raccolta e di successivo trattamento dei dati) e di tempestività.

registrando data, ora, autore e motivo dell'intervento, ambiente operativo interessato e i dati precedenti la modifica;

— i processi di acquisizione di dati da *information provider* esterni sono documentati e presidiati;

— i dati sono conservati con una granularità adeguata a consentire le diverse analisi e aggregazioni richieste dalle procedure di sfruttamento;

— i rapporti prodotti espongono le principali assunzioni e gli eventuali criteri di stima adottati (ad es., nell'ambito del monitoraggio dei rischi aziendali);

— il sistema di *reporting* consente di produrre informazioni tempestive e di qualità elevata per l'autorità di vigilanza e per il mercato.

SEZIONE VI

L'ESTERNALIZZAZIONE DEL SISTEMA INFORMATIVO

1. Tipologie di esternalizzazione

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale adottato: dall'*outsourcing* verticale (relativo a determinati processi operativi) all'*outsourcing* orizzontale di servizi trasversali come la gestione degli apparati hardware (*facility management*), lo sviluppo e la gestione del parco applicativo (*application management*), i collegamenti di rete, l'*help desk* tecnico e gli interventi di riparazione e manutenzione delle risorse ICT, fino al *full outsourcing* del complessivo sistema informativo aziendale.

Le norme nella presente Sezione si applicano ai casi di *full outsourcing* o di esternalizzazione di componenti critiche del sistema informativo, a complemento di quanto disposto in materia di *outsourcing* di funzioni aziendali nel Capitolo 3, Sezioni IV e V.

L'intermediario valuta la possibilità di ricorrere all'esternalizzazione considerando attentamente tutti i rischi (tra cui: operativi, di *compliance*, strategici e reputazionali) inerenti tale opzione, e tenendo conto della necessità, nel caso, di mettere in atto le idonee misure di contenimento.

Con particolare riferimento all'esternalizzazione di parte o tutto il sistema presso fornitori al di fuori del gruppo di appartenenza, la scelta è basata su un'analisi del rischio, che considera in primo luogo la stima dei rischi delle risorse e servizi da esternalizzare (ad es., tiene conto della classificazione dei dati e della criticità dell'operatività interessata, valutando in particolare i rischi derivanti dalla perdita del controllo diretto su componenti del sistema informativo e personale critici, nonché dei volumi delle operazioni) e quindi valuta i rischi dei possibili fornitori (ad es., condizioni finanziarie, posizionamento sul mercato, qualità e *turnover* del *management* e del personale, capacità di gestire la continuità operativa e di fornire accurati e tempestivi *report* direzionali sull'attività svolta, competenza ed esperienza, qualità e sicurezza nonché economicità e maturità, in un adeguato orizzonte temporale, della fornitura), la qualità dei sub-fornitori, la ridondanza delle linee di comunicazione utilizzate nonché l'affidabilità, la sicurezza e la scalabilità delle tecnologie adottate.

Nell'elaborazione del modello architetturale e delle strategie di esternalizzazione vanno considerati approcci tesi a contenere, per quanto possibile, il grado di dipendenza da specifici fornitori e partner tecnologici esterni al gruppo bancario (c.d. *vendor lock-in*), salvaguardando la possibilità di sostituire la fornitura con un'altra funzionalmente equivalente (ad es., privilegiando il ricorso a standard aperti per le connessioni, la memorizzazione e lo scambio di dati, la cooperazione applicativa) e prevedendo opportune *exit strategies* (1). Tali valutazioni tengono conto del principio di proporzionalità e dell'opportunità, per le banche di maggiore

(1) Anche l'acquisizione di licenze *software* per prodotti installati sul proprio sistema, a supporto di importanti processi aziendali trasversali, può introdurre forme di dipendenza dal fornitore, a seguito di vincoli tecnologici o contrattuali che impongano il ricorso al fornitore o a società collegate per la manutenzione o rendano assai ardua la sostituzione del prodotto. Tali considerazioni rientrano tra gli elementi essenziali nel processo di selezione delle soluzioni *software*.

dimensione, di mantenere all'interno della banca o del gruppo competenze professionali per gestire una transizione tra modelli di *sourcing* in caso di grave necessità.

Il mantenimento nel tempo da parte del fornitore delle condizioni necessarie a fornire un servizio rispondente alle esigenze e conforme alle norme è assicurato attraverso idonei strumenti contrattuali e procedure di controllo.

2. Accordi con i fornitori e altri requisiti

Nel caso di esternalizzazione del sistema informativo e di risorse ICT critiche, la comunicazione preventiva alla Banca centrale europea o alla Banca d'Italia (cfr. Capitolo 3, Sezioni IV e V) include i risultati dell'analisi dei rischi e – limitatamente agli intermediari delle macro-categorie 1 e 2 a fini SREP – la descrizione delle *exit strategies* previste.

Il referente per l'attività esternalizzata possiede le competenze idonee per esercitare il proprio ruolo di controllo sulle componenti gestite dal fornitore di servizi.

Nei contratti con i fornitori di sistemi e servizi ICT, in aggiunta alle richiamate disposizioni del Capitolo 3, sono disciplinati al minimo i seguenti aspetti:

— l'obbligo per il fornitore di servizi di osservare la *policy* di sicurezza informatica aziendale, per quanto applicabile; il fornitore provvede al trattamento dei dati in accordo con il loro livello di classificazione, con particolare riferimento alla riservatezza;

— la proprietà di dati, software, documentazione tecnica e altre risorse ICT, con l'esclusiva per l'intermediario sui dati inerenti la clientela e i servizi ad essa forniti;

— la periodica produzione delle copie di *backup* del sistema informativo (database, transazioni, log applicativi e di sistema); l'intermediario può accedere alle copie di *backup* su richiesta;

— la ripartizione dei compiti e delle responsabilità attinenti i presidi di sicurezza per la tutela di dati, applicazioni e sistemi; i presidi sono riferiti alle principali minacce interne ed esterne, anche attraverso canali digitali;

— le procedure di comunicazione e coordinamento in caso di incidenti di sicurezza informatica e di continuità operativa;

— la definizione di livelli di servizio coerenti con le esigenze delle applicazioni e dei processi aziendali che si avvalgono dei servizi esternalizzati;

— la predisposizione di misure di tracciamento idonee a garantire l'*accountability* e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati riservati;

— il raccordo con i ruoli e le procedure definite all'interno dell'intermediario per il processo di analisi dei rischi (cfr. Sezione III) e per il sistema di gestione dei dati (cfr. Sezione V);

— la possibilità per l'intermediario di conoscere l'ubicazione dei *data center* e una indicazione del numero di addetti con accesso ai dati riservati o alle componenti critiche; tali informazioni sono periodicamente aggiornate dal fornitore di servizi;

— l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare – facendo uso di opportuni strumenti e capacità tecniche, debitamente documentati – qualsiasi copia o stralcio di dati riservati di proprietà dell'intermediario e presente su propri sistemi o supporti, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi.

3. Indicazioni particolari

L'intermediario pone particolare cautela nella valutazione di iniziative di esternalizzazione a fornitori di servizi in *cloud computing* (servizi *cloud*), ossia un modello che consente l'accesso in rete diffuso, conveniente, flessibile e su richiesta, a un gruppo condiviso di risorse informatiche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere fornite e messe a disposizione rapidamente con un minimo di attività gestionale o di interazione con il fornitore del servizio.

Il *cloud computing* può essere realizzato secondo diverse tipologie:

— *cloud privato (private cloud)*: infrastruttura *cloud* disponibile per l'utilizzo esclusivo da parte di un solo ente;

— *cloud di comunità (community cloud):* infrastruttura *cloud* disponibile per l'utilizzo esclusivo da parte di una specifica comunità di enti, compresa una pluralità di enti appartenenti a un unico gruppo;

— *cloud pubblico (public cloud)*: infrastruttura *cloud* in cui i servizi sono erogati a un vasto numero di utenti con funzionalità offerte in maniera aperta e condivisa.

— *cloud ibrido (hybrid cloud)*: infrastruttura *cloud* costituita da due o più infrastrutture *cloud* distinte.

All'esternalizzazione del sistema informativo e di risorse ICT a fornitori di servizi *cloud*, gli intermediari applicano, nel rispetto di quanto previsto dalla presente Sezione e a integrazione di quanto disposto in materia di *outsourcing* di funzioni aziendali nel Capitolo 3, Sezioni IV e V, le "Raccomandazioni in materia di esternalizzazione a fornitori di servizi *cloud*", emanate dall'ABE.

SEZIONE VII

PRINCIPI ORGANIZZATIVI RELATIVI A SPECIFICHE ATTIVITÀ O PROFILI DI RISCHIO

1. Sicurezza dei servizi di pagamento

Le banche che prestano servizi di pagamento si attengono a quanto previsto dagli "Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2) (1) e dagli "Orientamenti finali sulla sicurezza dei pagamenti via internet" emanati dall'ABE (2) (3).

Gli Orientamenti integrano, per i profili relativi alla prestazione dei servizi di pagamento, le disposizioni organizzative concernenti gli assetti di governo e controllo previste dai Capitoli 3 e 4 del presente Titolo.

Ai fini dell'applicazione degli Orientamenti, le banche assicurano che:

— le politiche di governo dei rischi e il processo di gestione dei rischi (cfr. Cap. 3 Sez. II Par. 3) tengano conto dei rischi operativi e di sicurezza relativi ai servizi di pagamento e identifichino, in conformità con gli Orientamenti, le misure di controllo e di mitigazione adottate per tutelare adeguatamente gli utenti dei servizi di pagamento contro i rischi di sicurezza, compresi la frode e l'uso illegale di dati sensibili e personali;

— il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico e la gestione della sicurezza informatica, inclusa la *policy* di sicurezza informatica, sia integrato con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi e reputazionali), in modo da garantire una gestione e una valutazione unitarie dei rischi relativi alla prestazione dei servizi di pagamento. In particolare, a questo fine le banche:

  (a) integrano la classificazione delle risorse ICT in termini di criticità con quella delle funzioni delle attività e dei processi di supporto per la prestazione servizi di pagamento;

  (b) includono, nell'ambito delle verifiche delle misure di sicurezza (cfr. Cap. 4 Sez. IV Par. 3), le misure rilevanti per: i) i terminali ed i dispositivi utilizzati per la prestazione dei servizi di pagamento; ii) i terminali ed i dispositivi utilizzati per l'autenticazione degli utenti dei servizi di pagamento e iii) i dispositivi ed il *software* forniti dai prestatori di servizi di pagamento agli utenti per generare/ricevere un codice di autenticazione;

  (c) applicano le disposizioni per la gestione degli incidenti di sicurezza informatica, *mutatis mutandis*, alla gestione degli incidenti operativi relativi alla prestazione

(1) https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

(3) Per l'applicazione degli Orientamenti finali sulla sicurezza dei pagamenti via internet, cfr. inoltre le disposizioni transitorie previste dal par. 2.

dei servizi di pagamento, anche non collegati al funzionamento delle risorse e dei processi ICT. Le banche notificano alla Banca d'Italia i gravi incidenti operativi e di sicurezza relativi ai servizi di pagamento e trasmettono copia delle eventuali comunicazioni inviate (o che saranno inviate) alla clientela, non appena disponibili (4).

— il processo di analisi del rischio informatico sia coordinato e integrato con la valutazione annuale approfondita dei rischi operativi e di sicurezza relativi ai servizi di pagamento prestati e dell'adeguatezza delle misure di mitigazione e dei meccanismi di controllo messi in atto per affrontarli. Una relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento è trasmessa alla Banca centrale europea e alla Banca d'Italia, entro il 30 aprile di ogni anno.

— i processi e le misure volti a preservare la sicurezza delle informazioni garantiscano la riservatezza dei dati sensibili relativi ai pagamenti, siano essi inutilizzati, in transito o in uso. A tal fine, le procedure adottate per la progettazione, lo sviluppo e la prestazione dei servizi di pagamento garantiscono che le attività di raccolta, instradamento, trattamento, memorizzazione e/o archiviazione, nonché di visualizzazione dei dati sensibili relativi ai pagamenti siano adeguate, pertinenti e limitate a quanto strettamente necessario per la prestazione dei servizi stessi (5);

— il piano di continuità operativa di cui al Capitolo 4, Sezione II, par. 1, riporta, per i servizi di pagamento, le misure di mitigazione da adottare in caso di interruzione dei servizi critici e di cessazione dei contratti vigenti, al fine di evitare effetti negativi sul sistema bancario e finanziario e sugli utenti dei servizi di pagamento, nonché per garantire l'esecuzione delle operazioni di pagamento in corso.

2. Disposizioni transitorie

Le banche che prestano servizi di pagamento mediante uso del canale *internet* applicano le disposizioni degli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" secondo il regime transitorio delineato dall'ABE nella "*Opinion on the transition from PSD1 to PSD2*" del 19 dicembre 2017 e fino 14 settembre 2019, data di applicazione del Regolamento delegato della Commissione del 27 novembre 2017 n. 2018/389 riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE (PSD2).

(4) Cfr. Articolo 96, paragrafo 1, comma 2, della PSD2.

(5) Resta fermo il rispetto di altre disposizioni di legge aventi ad oggetto il trattamento dei dati personali (cfr. ad esempio, il Regolamento (UE) n. 2016/679 in materia di protezione dei dati personali).

Allegato A

DOCUMENTI AZIENDALI PER LA GESTIONE E IL CONTROLLO DEL SISTEMA INFORMATIVO

Documento	Approvazione	Aggiornamento	Note
DOCUMENTI DI *POLICY* E STANDARD AZIENDALI			
Documento di indirizzo strategico	Organo con funzione di supervisione strategica	In dipendenza della periodicità dei piani strategici aziendali (3 – 5 anni)	Contiene (cfr. Sezione II, par. 1): – modello di riferimento architetturale – strategie di *sourcing* – propensione al rischio informatico
Metodologia di analisi del rischio informatico	Organo con funzione di supervisione strategica	In base alla necessità	
Policy di sicurezza informatica	Organo con funzione di supervisione strategica	In base alla necessità	
Organigramma della funzione ICT	Organo con funzione di supervisione strategica	In base alla necessità	Include il disegno dei processi di gestione dell'ICT (cfr. Sezione II, par. 2)
Standard di *data governance*	Organo con funzione di gestione	Periodicità definita	
ALTRI DOCUMENTI ESSENZIALI PER LA GESTIONE E LO SVILUPPO DEI SISTEMI ICT			
Procedura di gestione dei cambiamenti	Organo con funzione di gestione	In base alla necessità	
Procedura di gestione degli incidenti	Organo con funzione di gestione	In base alla necessità	
Piano operativo	Organo con funzione di gestione	Annuale	
VALUTAZIONI AZIENDALI			
Rapporto sintetico su adeguatezza e costi dell'ICT	Organo con funzione di supervisione	Annuale	

Documento	Approvazione	Aggiornamento	Note
	strategica		
Rapporto sintetico sulla situazione del rischio informatico	Organo con funzione di supervisione strategica	Annuale	
Rapporti dell'*internal audit* e delle altre funzioni responsabili della valutazione della sicurezza	Organo con funzione di supervisione strategica	Almeno annuale	

TITOLO IV

Capitolo 5

LA CONTINUITÀ OPERATIVA

TITOLO IV – Capitolo 5

LA CONTINUITÀ OPERATIVA

1. Destinatari

L'Allegato A, Sezione II (Requisiti per tutti gli operatori) si applica alle banche e ai gruppi bancari.

L'Allegato A, Sezione III (Requisiti particolari per i processi a rilevanza sistemica) si applica, in aggiunta ai requisiti previsti nella Sezione II dell'Allegato A, ai soggetti, individuati nominativamente, con apposita comunicazione, fra i gruppi bancari e le banche non appartenenti a gruppi con una quota di mercato, calcolata sul totale attivo, superiore al 5 per cento del totale del sistema bancario.

Nell'ambito dei gruppi bancari, i requisiti particolari si applicano alla capogruppo, alle singole controllate bancarie italiane con totale attivo superiore a 5 miliardi di euro e alle altre controllate bancarie, finanziarie e strumentali che, indipendentemente dalla dimensione e localizzazione, svolgono in misura rilevante i processi a rilevanza sistemica o danno un supporto essenziale a questi ultimi.

Possono essere altresì assoggettati ai requisiti particolari gli operatori, incluse le succursali italiane di banche estere, che, su base individuale, detengono una quota di mercato superiore al 5 per cento in almeno uno dei seguenti segmenti del sistema finanziario italiano: regolamento lordo in moneta di banca centrale, liquidazione di strumenti finanziari, servizi di controparte centrale, sistemi multilaterali di scambio di depositi interbancari in euro, aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, mercato dei pronti contro termine all'ingrosso su titoli di Stato, pagamento delle pensioni sociali, bollettini postali.

2. Fonti normative

La materia è regolata dalle seguenti disposizioni del TUB:

- art. 51, il quale prevede che le banche inviino alla Banca d'Italia, con le modalità e i tempi da essa stabiliti, le segnalazioni periodiche nonché ogni dato e documento richiesti;
- art. 53, comma 1, lett. d), che attribuisce alla Banca d'Italia il potere di emanare disposizioni di carattere generale in materia di organizzazione amministrativa e contabile e controlli interni delle banche;
- art. 67, comma 1, lett. d), il quale prevede che, al fine di esercitare la vigilanza consolidata, la Banca d'Italia impartisca alla capogruppo, con provvedimenti di carattere generale, disposizioni concernenti il gruppo complessivamente considerato o i suoi componenti aventi ad oggetto l'organizzazione amministrativa e contabile e i controlli interni;

e inoltre:

- dalla delibera del CICR del 2 agosto 1996, come modificata dalla delibera del 23 marzo 2004, in materia di organizzazione amministrativa e contabile e controlli interni delle banche e dei gruppi bancari;
- dal decreto legislativo 27 gennaio 2010, n. 11, Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE, e successive modifiche e integrazioni.

Vengono inoltre in rilievo:

- la CRD IV;
- la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n.1093/2010, e abroga la direttiva 2007/64/CE (PSD2);
- gli Orientamenti finali sulla sicurezza dei pagamenti via Internet, emanati dall'ABE il 19 dicembre 2014 ([1]);
- gli Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2), emanati dall'ABE il 12 gennaio 2018 ([2]).

Si tiene anche conto delle *Guidelines on Internal Governance*, dell'EBA/CEBS del 27 settembre 2011.

3. Banche soggette ai requisiti applicabili a tutti gli operatori (Allegato A, Sezione II)

Fermo restando quanto previsto nell'Allegato A, Sezione II, si precisa quanto segue:

- i gruppi bancari - coerentemente con quanto previsto nel Capitolo 3, Sezione V (il RAF, il sistema dei controlli interni e l'esternalizzazione nei gruppi bancari) – possono definire e gestire i piani di continuità operativa in modo accentrato per l'intero gruppo o decentrato per singola società. In ogni caso la capogruppo assicura che tutte le controllate siano dotate di piani di continuità operativa e verifica la coerenza degli stessi con gli obiettivi strategici del gruppo in tema di contenimento dei rischi. A livello di gruppo sono stabiliti controlli sul raggiungimento degli obiettivi di continuità operativa definiti per l'intero gruppo e le singole componenti;
- i compiti e le responsabilità degli organi aziendali indicati ai punti a), b), c), d), ed e) dell'Allegato A, Sezione II, par. 3.1, rientrano nelle competenze dell'organo con funzione di supervisione strategica; i compiti e le responsabilità indicati nei punti f) e g) del menzionato paragrafo, spettano all'organo con funzione di gestione;
- le banche segnalano alla Banca d'Italia, tra le "cariche rilevanti a fini di Vigilanza" previste nella procedura "organi sociali" (Or.So.), il nome del responsabile del piano di continuità operativa (cfr. Allegato A, Sezione II, par. 0);

Formattato:

([1]) https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2

([2]) EBA/GL/2017/17.

- la procedura per la dichiarazione dello stato di crisi (cfr. Allegato A, Sezione II, par. 3.1) è definita in raccordo con il processo di gestione degli incidenti di sicurezza informatica (cfr. Capitolo 4, Sezione IV, par. 6) e delle altre tipologie di incidenti;
- le verifiche annuali dei sistemi informativi (cfr. Allegato A, Sezione II, par. 3.5) prevedono anche l'operatività *on-line* di almeno una succursale;
- le previsioni in materia di Esternalizzazione, infrastrutture e controparti rilevanti (cfr. Allegato A, Sezione II, par. 3.7), si applicano coerentemente con quanto previsto dalle disposizioni in materia di esternalizzazione previste nei Capitoli 3 e 4;
- in caso di situazione di crisi che non assumano rilevanza sistemica per il sistema finanziario, le banche e i gruppi bancari contattano, al fine di agevolare il coordinamento degli interventi, la Banca d'Italia e alla Banca centrale europea.

4. Banche soggette ai requisiti particolari per i processi a rilevanza sistemica (Allegato A, Sezione III)

Fermo restando quanto previsto nell'Allegato A, Sezione III, si precisa quanto segue:

per i gruppi bancari, la capogruppo promuove e coordina l'attuazione degli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica e garantisce nel continuo il rispetto da parte di tutte le controllate interessate dei requisiti previsti per i processi a rilevanza sistemica. Nomina un responsabile unico di tali attività, con competenze estese all'intero gruppo (cfr. Allegato A, Sezione III, par. 2.2);

per le succursali italiane di intermediari esteri, il coordinamento del piano di continuità operativa relativo ai processi a rilevanza sistemica è assicurato dalle succursali stesse, in stretto raccordo con le strutture che gestiscono la continuità operativa a livello centrale o di area geografica.

ALLEGATO A

REQUISITI PER LA CONTINUITÀ OPERATIVA

SEZIONE I

DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio richiedono che gli operatori rafforzino l'impegno a garantire adeguati livelli di continuità operativa.

A tal fine, essi adottano un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di continuità operativa commisurati ai livelli di rischio.

Le concrete misure da adottare tengono conto degli standard e *best practices* definiti a livello internazionale e/o definiti nell'ambito degli organismi di categoria.

2. 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 o a rilevanza sistemica 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 e a rilevanza sistemica. Esso è generalmente articolato in piani settoriali;

— "*piano di disaster recovery*": documento che stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il

piano di *disaster recovery*, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa;

— "*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 propri processi critici e a rilevanza sistemica, anche in caso di incidenti o disastri che rendano indisponibile il sito primario;

— "*sito primario*": infrastruttura presso la quale sono normalmente svolte le attività dell'operatore;

— "*tempo di ripristino di un processo*": periodo che intercorre fra il momento in cui l'operatore dichiara lo stato 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;
- 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.

SEZIONE II

REQUISITI PER TUTTI GLI OPERATORI

1. Ambito del piano di continuità operativa ([1])

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 fornitori; clientela primaria; specifici mercati finanziari; sistemi di regolamento, compensazione e garanzia).

I piani di continuità operativa prevedono soluzioni, non solo basate su misure tecnico-organizzative finalizzate alla salvaguardia degli archivi elettronici e al funzionamento dei sistemi informativi, ma che considerino anche ipotesi di crisi estesa e blocchi prolungati delle infrastrutture essenziali in modo da assicurare la continuità operativa dell'operatore in caso di eventi disastrosi.

Laddove alcuni processi critici siano svolti da soggetti specializzati appartenenti al gruppo (ad es., allocazione della funzione informatica o del *back-office* presso una società strumentale), i relativi presidi di continuità operativa costituiscono parte integrante dei piani di continuità operativa degli operatori.

Il piano di continuità operativa si inquadra nella complessiva politica di governo dei rischi dell'operatore; esso tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali.

Il piano di continuità operativa prende in considerazione diversi scenari di crisi basati almeno sui seguenti fattori di rischio, conseguenti a eventi naturali o attività umana, inclusi danneggiamenti gravi da parte di dipendenti:

— distruzione 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 critici.

Il piano di continuità operativa indica le procedure per il rientro dall'emergenza, con particolare attenzione alla rilevazione dei danni, alla gestione di tutte le operazioni di rientro, alla verifica dell'operatività per i servizi ripristinati.

([1]) Con riferimento alla prestazione dei servizi di pagamento, le banche si attengono inoltre a quanto previsto dagli Orientamenti dell'EBA sulla sicurezza dei pagamenti via Internet e sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento, come recepiti nel Capitolo 4, Sezione VII.

2. Analisi di impatto

L'analisi di impatto, preliminare alla stesura del piano di continuità operativa e periodicamente aggiornata ([2]), individua il livello di rischio relativo ai singoli processi aziendali e pone in evidenza le conseguenze della interruzione del servizio. I rischi residui, non gestiti dal piano di continuità operativa, sono documentati ed esplicitamente 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, 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*);

— l'assetto organizzativo in termini di accentramento o decentramento di processi critici;

— i vincoli derivanti da interdipendenze, anche tra e con fornitori, 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).

3. Definizione del piano di continuità operativa e gestione delle crisi

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;

([2]) 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.

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 di continuità operativa;

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 di continuità operativa;

f) promuove lo sviluppo, il controllo periodico del piano di continuità operativa e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti;

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.

3.2 I processi critici

Gli operatori identificano in modo circostanziato i processi 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.

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, 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 e collabora attivamente alla realizzazione delle misure di continuità operativa.

3.3 La 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. Tale figura tiene inoltre i contatti con la Banca d'Italia e con la Banca centrale europea in caso di crisi.

Laddove il piano di continuità operativa sia articolato in piani settoriali, gli operatori individuano i referenti per ciascuno di essi. I referenti dei piani settoriali (3) coordinano, per gli aspetti di competenza, i lavori per la definizione e la manutenzione dei piani, per l'attuazione delle misure previste nello stesso e per la conduzione delle verifiche. Prima dell'attivazione di nuovi sistemi o processi operativi, essi definiscono le opportune modifiche dei piani.

3.4 Il 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 di continuità operativa 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 assunta 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 esplicitamente 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.

Il piano di continuità operativa individua i siti alternativi, prevede spazi e infrastrutture logistiche e di comunicazione adeguate per il personale coinvolto nella crisi, stabilisce le regole di conservazione delle copie dei documenti importanti (ad es., i contratti) in luoghi remoti rispetto ai documenti originali.

Con riferimento ai sistemi informativi centrali e periferici, il piano di continuità operativa integra il piano di *disaster recovery* (4). In quest'ultimo sono fornite indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione, nonché sulle procedure per il ripristino presso i siti alternativi.

La frequenza dei *back-up* è correlata alle dimensioni e alle funzioni (5) dell'operatore; gli archivi di produzione dei processi critici sono duplicati almeno giornalmente. Sono assunte cautele per il tempestivo trasporto e la conservazione delle copie elettroniche in siti a elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione (6).

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

---

(3) Ove il piano di continuità operativa non sia articolato in piani settoriali, tali attività sono svolte dal responsabile del piano di continuità operativa.

(4) In caso di *outsourcing* di componenti critiche del sistema informativo si applica quanto indicato al par. 3.7.

(5) Ad esempio, nel caso in cui svolga il ruolo di tramite per partecipanti indiretti.

(6) Per i processi non critici sono comunque realizzati 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 definite modalità e tempi per l'allineamento con i sistemi di produzione dopo il loro ripristino.

I siti alternativi possono dover essere utilizzati, in caso di necessità, anche per periodi prolungati.

3.5 Le verifiche

Gli intermediari sottopongono a verifica annuale i piani per la continuità operativa delle funzioni, dei servizi, dei sistemi, delle transazioni e delle interdipendenze riferite ai processi critici.

Le modalità di verifica delle misure di continuità operativa dipendono dalla criticità dei processi e dai rischi ravvisati; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'incidente o della catastrofe che può causare la crisi; per i processi critici le verifiche prevedono il coinvolgimento degli utenti finali, dei fornitori di servizi e, qualora possibile, delle controparti rilevanti.

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.

In particolare, le verifiche annuali dei sistemi informativi prevedono l'attivazione dei collegamenti di rete presso il sito alternativo e l'esecuzione delle procedure *batch* con controllo della funzionalità e delle prestazioni dei siti alternativi. Le prove sono preferibilmente realizzate con dati di produzione.

I risultati delle verifiche sono documentati per iscritto, portati all'attenzione degli organi aziendali competenti e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di *audit*. A fronte di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive.

3.6 Le risorse umane

Il piano di continuità operativa individua il personale essenziale per assicurare la continuità operativa dei processi critici e fornisce allo stesso 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 nei processi cui si riferiscono.

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

3.7 Esternalizzazione, infrastrutture e controparti rilevanti

In caso di esternalizzazione di funzioni aziendali connesse allo svolgimento di processi critici, il piano di continuità operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore o sul fornitore di servizi.

Nel contratto sono formalizzati i livelli di servizio assicurati in caso di crisi e le soluzioni di continuità operativa poste in atto dal fornitore di servizi, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

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

Il piano di continuità operativa dell'operatore considera l'eventualità che le principali infrastrutture tecnologiche e 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 i siti alternativi di tali soggetti è verificata periodicamente.

Per i servizi essenziali dell'operatore, va valutata la possibilità di prevedere il ricorso, in casi di emergenza, a fornitori alternativi.

Nel caso in cui il fornitore 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.

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 di continuità operativa 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 anche coinvolta nel controllo dei piani di continuità operativa dei fornitori di servizi esternalizzati e degli altri fornitori critici; 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.

3.9 Comunicazioni alla Banca d'Italia e alla Banca centrale europea

In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia e alla Banca centrale europea valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

SEZIONE III

REQUISITI PARTICOLARI PER I PROCESSI A RILEVANZA SISTEMICA

1. Premessa

L'operatività del sistema finanziario nel suo complesso si basa sul corretto funzionamento dei maggiori operatori e sulla loro capacità di erogare i servizi essenziali nei comparti dei sistemi di pagamento e dell'accesso ai mercati finanziari.

A tali soggetti la Banca d'Italia può chiedere il rispetto di requisiti di continuità operativa più stringenti rispetto a quelli previsti per la generalità degli operatori, in particolare con riferimento ai tempi di ripristino per i processi a rilevanza sistemica (cfr. par. 2.1), alla localizzazione dei siti alternativi, alle risorse previste per gestire le situazioni di crisi.

La Banca d'Italia individua nominativamente gli operatori ai quali si applicano i requisiti particolari, richiede adeguamenti dei piani di continuità operativa, verifica le soluzioni adottate. Tali operatori partecipano alle iniziative per il coordinamento della continuità operativa del sistema finanziario del CODISE.

2. Definizione del piano di continuità operativa e gestione delle crisi

2.1 Processi a rilevanza sistemica

I processi ad alta criticità nel sistema finanziario italiano che, per un effetto di contagio, possono provocare il blocco dell'operatività dell'intera piazza finanziaria nazionale si concentrano nei sistemi di pagamento e nelle procedure per l'accesso ai mercati finanziari.

Tali processi sono denominati, ai fini delle presenti disposizioni, "processi a rilevanza sistemica" per la continuità operativa del sistema finanziario italiano. La Banca d'Italia comunica a ciascun operatore i processi a rilevanza sistemica di pertinenza. Si tratta di un complesso strutturato di attività finalizzate all'erogazione dei seguenti servizi:

— servizi connessi con i sistemi di regolamento lordo in moneta di banca centrale e con i sistemi di gestione accentrata, compensazione, garanzia e liquidazione degli strumenti finanziari. Sono inclusi: regolamento lordo in moneta di banca centrale (Target 2), liquidazione di strumenti finanziari (Express II), gestione accentrata di strumenti finanziari, sistemi di riscontro e rettifica giornalieri, servizi di controparte centrale;

— servizi connessi con l'accesso ai mercati rilevanti per regolare la liquidità del sistema finanziario. Sono inclusi: sistemi multilaterali di scambio di depositi interbancari in euro (e-Mid), aste BCE, operazioni di finanziamento del Tesoro effettuate tramite asta, Mercato dei pronti contro termine all'ingrosso su titoli di Stato (MTS comparto PCT);

— servizi di pagamento al dettaglio a larga diffusione tra il pubblico. Sono inclusi: bollettini postali, pagamento delle pensioni sociali, erogazione del contante;

— servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull'operatività degli

stessi. Sono inclusi: gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM, supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).

2.2 Responsabilità

L'operatore:

— attua gli interventi di adeguamento dei piani di continuità operativa relativi ai processi a rilevanza sistemica;

— garantisce nel continuo il rispetto dei requisiti particolari;

— nomina un responsabile unico di tali attività.

2.3 Scenari di rischio

Gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica sono documentati e costantemente aggiornati. Essi includono, in aggiunta a quanto previsto per tutti gli operatori: eventi catastrofici con distruzioni fisiche su larga scala, a dimensione metropolitana o superiore, che investano infrastrutture essenziali dell'operatore e di terzi; situazioni di crisi gravi anche non connesse ad eventi con distruzioni materiali (ad es., pandemie, attacchi biologici, attacchi informatici su larga scala).

2.4 Siti alternativi

I siti alternativi per i processi a rilevanza sistemica sono situati a congrua distanza dai siti primari in modo da assicurare un elevato grado di indipendenza tra i due insediamenti.

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 necessaria 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.

2.5 Tempi di ripristino e percentuali di disponibilità

Il tempo di ripristino per i processi a rilevanza sistemica non supera le quattro ore. Il tempo di ripartenza per i processi a rilevanza sistemica non supera le due ore.

Se un evento catastrofico che colpisce un operatore determina un blocco dei processi a rilevanza sistemica di altri operatori, questi ultimi ripristinano i propri processi sistemici entro due ore dalla ripartenza dell'operatore colpito in prima istanza.

Nel caso in cui gli scenari (cfr. par. 2.3) determinino impatti particolarmente gravi, gli obiettivi di ripristino indicati possono subire un adattamento che sarà segnalato agli operatori interessati dalla Banca d'Italia, tenuto conto delle indicazioni 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 l'intervallo di tempo che intercorre fra il punto di ripristino e il momento dell'incidente è pari o prossimo a zero.

E' previsto, anche in caso di situazioni estreme, un ripristino quanto più possibile immediato dei processi a rilevanza sistemica, 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*, fax, contatti telefonici con controparti selezionate), in particolare per gestire le esigenze essenziali di liquidità.

2.6 Risorse

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

2.7 Verifiche

Sono effettuate, con frequenza almeno annuale, verifiche accurate sui presidi delle misure di continuità operativa dei processi a rilevanza sistemica. Viene assicurata la partecipazione attiva ai test e alle simulazioni di sistema organizzati o promossi dalle autorità, dai mercati e dalle principali infrastrutture finanziarie.

3. Comunicazioni alla Banca d'Italia e alla Banca centrale europea

In caso di incidenti che possano avere impatti rilevanti sui processi a rilevanza sistemica, la dichiarazione dello stato di crisi prevede l'immediata richiesta di attivazione del CODISE con una prima valutazione degli operatori potenzialmente danneggiati.

In caso di crisi, successivamente al ripristino dei processi a rilevanza sistemica, l'operatore fornisce con tempestività alla Banca d'Italia e alla Banca centrale europea valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

Gli operatori sistemici inviano alla Banca d'Italia e alla Banca centrale europea 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.