Policy di Continuità Operativa del Conglomerato Finanziario Mediolanum

Consiglio di Amministrazione di Banca Mediolanum S.p.A. del 19 dicembre 2023

INDICE

1. AMBITO DEL DOCUMENTO

Banca Mediolanum S.p.A., Capogruppo del Conglomerato Finanziario Mediolanum (di seguito anche Conglomerato Finanziario), è da sempre impegnata nel promuovere, all'interno della propria realtà aziendale e nei confronti dei propri dipendenti, una cultura aziendale conforme alle normative vigenti, allineata alle *best practice* di mercato ed in grado di garantire la soddisfazione delle proprie risorse e l'attenzione rivolta ai propri clienti.

La reputazione del Conglomerato e la propria integrità organizzativa sono considerati requisiti fondamentali per operare con successo all'interno del settore dei servizi bancari, finanziari ed assicurativi.

Il sistema di gestione della continuità operativa rappresenta un elemento chiave nel presidio del rischio reputazionale e nella gestione dei processi di Banca Mediolanum e di ciascuna Società del Conglomerato nei rapporti con la propria clientela ed il mercato.

Scopo della presente Policy è descrivere i principi adottati da Banca Mediolanum S.p.A. (nel seguito del documento anche "Banca Mediolanum" o "la Banca" o "la Capogruppo") per il presidio del modello, dei processi e delle procedure finalizzate alla continuità operativa del Conglomerato.

Il modello organizzativo predisposto risponde all'esigenza di gestire due differenti ambiti:

I. **Governo della Continuità Operativa** (o Governo del BCM – Business Continuity Management), che ha lo scopo di garantire l'adeguatezza delle strutture organizzative preposte a fronteggiare situazioni di crisi, riducendo a livelli ritenuti accettabili gli impatti conseguenti ad eventi disastrosi, attraverso la predisposizione ed il mantenimento di:
    - Piano di Continuità Operativa (Business Continuity Plan o BCP);
    - Processi di coordinamento con soggetti esterni coinvolti nella gestione di processi critici;

- Processi annuali di aggiornamento del perimetro dei processi critici e dello stato di funzionamento delle procedure adottate;
- Procedure operative per la gestione della crisi, oltre che per il rientro alla normalità.

II. **Gestione della Crisi**, che ha lo scopo di garantire una risposta immediata ad una crisi, assicurare che i piani di continuità e di ripristino siano attivati come previsto e fornire l'adeguato supporto gestionale affinché tali piani siano efficacemente applicati, fino al superamento della crisi e al ripristino di condizioni di normalità.

Le disposizioni in materia di Continuità Operativa evidenziano le sinergie tra le attività di analisi dei processi organizzativi, di gestione del rischio informatico, di business continuity e, più in generale, di gestione del rischio aziendale.

1.1. CONTESTO DI RIFERIMENTO

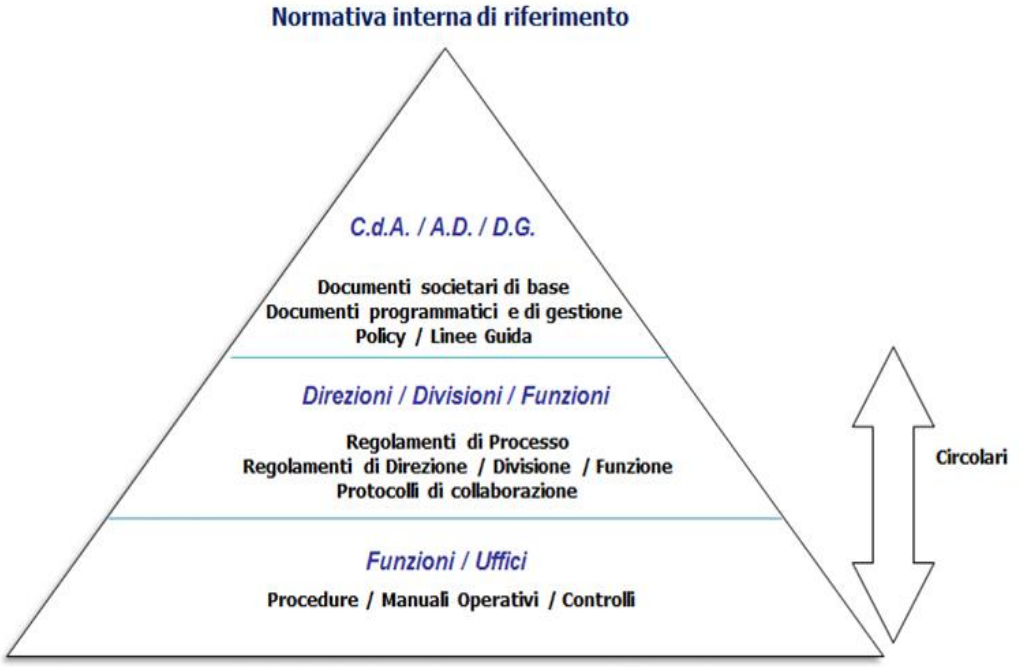
Nella più ampia logica del Sistema dei Controlli Interni il regolatore nazionale disciplina, nella Circolare di Banca d'Italia n.285 del 17 dicembre 2013 e successivi aggiornamenti - Disposizioni di Vigilanza per le Banche e successivi aggiornamenti nella Parte Prima, Titolo IV, Cap.5 - una sezione specifica denominata "La continuità operativa[1]". Le disposizioni disciplinano gli aspetti di carattere procedurale e organizzativo della Continuità Operativa per le Banche e i Gruppi Bancari, al fine di gestire i processi critici coerentemente al generale approccio al rischio di impresa.
La materia della continuità operativa è inoltre disciplinata per il settore assicurativo, per l'intermediazione finanziaria e per gli istituti di moneta elettronica rispettivamente dal Regolamento n. 38 di IVASS recante disposizioni in materia di sistema di governo societario per le Società Assicurative, dalla circolare n. 288 di Banca d'Italia recante disposizioni di Vigilanza per gli Intermediari Finanziari e dalle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emanate da Banca d'Italia in ultimo aggiornamento con provvedimento del 23 luglio 2019, nonché dalla regolamentazione locale applicabile alle Controllate estere.

[1] Banca d'Italia – Circolare n.285 – Disposizioni di Vigilanza per le Banche – Parte I, Titolo IV, Capitolo 5 "La continuità operativa"

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio richiedono, infatti, 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 practice* definiti a livello internazionale e/o definiti nell'ambito degli organismi e associazioni di categoria.

1.2. GERARCHIA DELLE FONTI

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente.



I principi richiamati nella presente policy trovano quindi attuazione nel Business Continuity Plan, nelle procedure operative e nei regolamenti di processo, nei quali

saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative.

2. APPLICABILITÀ

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Banca Mediolanum S.p.A. e trova diretta applicazione all'interno della Banca. I principi definiti si applicano a tutte le unità organizzative della Banca incluse nel perimetro di intervento.

Tale documento si applica alla Capogruppo Banca Mediolanum S.p.A. ed è trasmesso alle altre Società appartenenti al Conglomerato Finanziario Mediolanum che lo applicheranno, in base ad un principio di proporzionalità, per quanto da esse recepito nei rispettivi ordinamenti interni nonché, per le Società estere, per quanto compatibile con la legislazione del Paese di appartenenza.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità della Direzione Portafoglio Progetti e Sviluppo Organizzativo, all'interno della quale opera il Business Continuity Office.

3. DEFINIZIONI

Ai fini della presente Policy si intendono per:

- **Business Continuity**: capacità dell'azienda di continuare ad esercitare il proprio business a fronte di eventi avversi che possono colpirla; insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità a livelli predefiniti;
- **Crisi**: situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici o di 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 raggiungere, ove necessario, l'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 di rilevanza sistemica e può essere 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 è finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, e 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;
- **Obiettivo di punto di ripristino (Recovery Point Objective – RPO)**: il periodo massimo durante il quale è accettabile che i dati vadano persi in caso di incidente;
- **Sito alternativo**: infrastruttura che consente all'operatore di continuare a svolgere i propri processi critici 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 (Recovery Time Objective – RTO)**: periodo che intercorre tra il momento in cui l'operatore dichiara lo stato di crisi

e l'istante in cui il processo è ripristinato a un livello di servizio predefinito. Esso è costituito dai tempi di:

  - Analisi degli eventi e decisione delle azioni da intraprendere, prima di effettuare gli interventi;
  - 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;

- **Esternalizzazione**: l'accordo in qualsiasi forma tra una banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività che sarebbe altrimenti svolto dalla stessa banca;
- **Fornitore di servizi**: soggetto terzo che realizza, in tutto o in parte, un processo, un servizio o un'attività esternalizzata nell'ambito di un accordo di esternalizzazione;
- **Servizi ICT**: servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono, ad esempio: servizi di inserimento, archiviazione, elaborazione e comunicazione di dati, servizi di monitoraggio, di supporto alle attività e alle decisioni aziendali;
- **Soggetto terzo**: soggetto o organizzazione che ha stretto rapporti commerciali o stipulato contratti con una banca per la fornitura di un prodotto o un servizio;

4. RUOLI E RESPONSABILITÀ

A livello di Conglomerato Finanziario è previsto un modello di gestione "misto" della continuità operativa ovvero di:

- **Gestione accentrata** presso Banca Mediolanum del Piano di Continuità Operativa delle Controllate italiane del Conglomerato Finanziario e delle iniziative ad esso collegate, attraverso il BC Office di Capogruppo che svolge tale attività anche in outsourcing per le citate Controllate.

- **Gestione decentrata** per le Società Controllate del Conglomerato Finanziario con sede estera, alle quali è chiesto di attivare idonei presidi di gestione della

Continuità Operativa oltre che di prevedere flussi informativi periodici verso le funzioni della Capogruppo. Per tali Società è richiesta l'adozione di procedure di Continuità Operativa per le quali sarà applicato un principio di proporzionalità nelle procedure di gestione della crisi.

È inoltre costituito presso la Capogruppo un Comitato gestionale di Business Continuity, consultivo per le opportune decisioni della Banca e delle Società Controllate del Conglomerato Finanziario, che esprime a queste ultime eventuali pareri vincolanti e non vincolanti, al fine di assicurare adeguati presidi di Continuità Operativa a livello di Conglomerato; a tal fine possono partecipare al Comitato anche esponenti delle Controllate aventi gli opportuni poteri decisionali.
In modo analogo è costituito presso la Capogruppo anche un Comitato manageriale di Gestione della Crisi, al fine di garantire il governo integrato dei presidi da attivare in situazione di Crisi.

Il modello organizzativo per il presidio della continuità operativa è adottato sulla base dei principi descritti nel successivo paragrafo 5.2 e dettagliato nel Business Continuity Plan, Volume 1.

5. PRINCIPI IN TEMA DI GESTIONE DELLA CONTINUITÀ OPERATIVA

La definizione di una policy di Conglomerato Finanziario ha l'obiettivo di:

I. Richiamare i principi chiave di gestione e controllo della Continuità Operativa di Banca Mediolanum;
II. Fornire indicazioni alle Controllate circa i requisiti minimi previsti per la gestione della Continuità Operativa, tenendo conto dei principi di proporzionalità, oltre che della rilevanza dei processi svolti dalle medesime;
III. Definire standard di Conglomerato Finanziario a cui ispirarsi, che tengano conto di *best practice* internazionali;
IV. Richiamare i principi alla base delle esigenze di coordinamento tra le attività di analisi e presidio dei processi aziendali, dei sistemi informatici a supporto e le

attività di gestione della continuità operativa, alla luce della rilevanza della tecnologia nella gestione dei processi in ambito.

I principi alla base dei processi di gestione della continuità operativa del Conglomerato Finanziario sono stati raggruppati in 4 macro-ambiti:

- Principi generali;
- Principi organizzativi;
- Principi di funzionamento;
- Principi di *Business Continuity* in caso di ricorso a soggetti esterni per la prestazione di servizi ICT, esternalizzazione, infrastrutture e controparti rilevanti.

5.1 PRINCIPI GENERALI

- Le Società del Conglomerato Finanziario definiscono un Piano di Continuità Operativa per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale ovvero di catastrofi estese che colpiscono l'operatore o le sue controparti rilevanti:
- Il Piano di continuità operativa prevede 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.
- Il Piano di Continuità Operativa si inquadra nella complessiva politica di governo dei rischi;
- Il Piano di Continuità Operativa tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali;
- Il Piano è documentato, messo a disposizione delle unità operative (*business unit*) e di supporto e immediatamente accessibile in caso di emergenza. Inoltre, esso è aggiornato con cadenza almeno annuale sulla base dei risultati delle

verifiche, delle informazioni sulle minacce esistenti e dell'esperienza maturata in occasione di eventi precedenti[2].

- Il Piano di Continuità Operativa prende in considerazione diversi scenari di crisi, che devono includere almeno uno scenario di attacco informatico e considerare almeno i 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, anche con riferimento ai sistemi funzionali alla prestazione dei servizi di pagamento;
    - 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 deve prevedere anche scenari per l'attivazione del Disaster Recovery, che sarà adeguatamente documentato al fine di garantire la gestione integrata degli scenari sia dal punto di vista procedurale che di soluzioni tecnico-informatiche;
- Il Piano di Continuità Operativa è integrato dal piano di Disaster Recovery con riferimento ai sistemi informativi centrali e periferici;
- Gli scenari di crisi identificati nel Piano di Continuità Operativa tengono conto anche delle caratteristiche morfologiche del territorio (sismicità, vicinanza a corsi d'acqua, ecc.) o di location (vicinanza ad aree sensibili per eventuali attacchi terroristici o di sicurezza) proprie della Società e dei principali fornitori dei processi critici;
- 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

[2] Nell'aggiornamento dei piani di continuità operativa, le Società considerano anche le modifiche delle funzioni aziendali, dei processi e delle risorse informatiche di supporto nonché dei tempi di ripristino e degli obiettivi di punto di ripristino.

conseguenti; la capacità di comunicare con i siti alternativi di tali soggetti è verificata periodicamente;

- Il Piano di Continuità Operativa documenta i presupposti e le modalità di dichiarazione dello stato di crisi, l'organizzazione e le procedure da seguire in situazione di crisi, l'iter di ripresa della normale operatività;
- Il Piano di Continuità Operativa e il relativo processo di aggiornamento sono oggetto di verifica regolare da parte della funzione Internal Auditing. Tale funzione prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, propone modifiche al piano di continuità operativa sulla base delle mancanze riscontrate;
- In caso di crisi, successivamente al ripristino dei processi critici, l'operatore fornisce alla Banca d'Italia, alla Banca Centrale Europea e/o altre autorità di vigilanza di settore le valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

5.2 PRINCIPI ORGANIZZATIVI

- Le Società del Conglomerato Finanziario si dotano di processi e procedure idonei alla gestione degli scenari di crisi identificati e forniscono aggiornamento periodico alla Capogruppo sia in sede di aggiornamento della normativa interna che con riferimento all'esito delle verifiche periodicamente condotte.
- Il Consiglio di Amministrazione di ciascuna Società del Conglomerato, con il supporto della Direzione Generale laddove presente, valuta le misure tecnico-organizzativo adottate per la salvaguardia dei processi critici. In particolare:
    - Stabilisce gli obiettivi e le strategie di continuità operativa del servizio;
    - Assicura risorse umane, tecnologiche e finanziarie adeguate al conseguimento degli obiettivi fissati;
    - Approva il piano di continuità operativa e le successive modifiche a seguito di adeguamenti tecnologici e organizzativi, accettando i rischi residui non gestiti dal piano di continuità operativa;
    - È informato con frequenza almeno annuale, sugli esiti dei controlli sull'adeguatezza del piano, nonché sulle verifiche delle misure di continuità operativa;
    - 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;
    - 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'Alta Direzione definisce gli scenari a rischio, con l'ausilio delle funzioni specialistiche preposte alla gestione della continuità operativa e identifica le priorità di piani di intervento per la messa in sicurezza dei processi critici.

- Le Società del Conglomerato Finanziario identificano un Responsabile della Continuità Operativa e un Responsabile della Disaster Recovery che collaborano alla gestione coordinata dei Piani di Business Continuity e Disaster Recovery. Il Responsabile della Continuità Operativa e il Responsabile del Disaster Recovery di Banca Mediolanum sono nominati dal Consiglio di Amministrazione di Banca Mediolanum.
- Il Responsabile della Continuità Operativa ha una posizione gerarchico funzionale adeguata. In particolare:
    - Cura lo sviluppo del piano di continuità operativa, ne assicura l'aggiornamento nel continuo, a fronte di cambiamenti organizzativi e tecnologici rilevanti, ne verifica l'adeguatezza con cadenza almeno annuale;
    - Tiene i contatti con la Banca d'Italia e la Banca Centrale Europea e/o le altre autorità di vigilanza in caso di crisi.
- Le Società del Conglomerato Finanziario definiscono le procedure di Continuità Operativa a fronte di scenari di crisi coerentemente ad un principio di proporzionalità.
- Le Società del Conglomerato Finanziario allocano risorse per la gestione della crisi e prevedono priorità di intervento nella gestione della stessa coerenti al livello di rischio dei processi aziendali.
- L'attività svolta dagli organi aziendali coinvolti nel processo di gestione della continuità operativa e le decisioni assunte sono adeguatamente documentate.
- Nella gestione della crisi sono previste misure di escalation rapide, che consentano, una volta assunta consapevolezza della portata dell'incidente, di dichiarare la crisi in tempi brevi.

5.3 PRINCIPI DI FUNZIONAMENTO

- Le Società del Conglomerato Finanziario conducono periodicamente un'analisi di impatto, preliminare alla stesura e aggiornamento del piano di continuità operativa, che individua il livello di rischio relativo ai singoli processi aziendali sulla base di un approccio quantitativo e qualitativo e pone in evidenza le conseguenze dell'interruzione del servizio.
- Le Società considerano il grado di criticità delle funzioni aziendali, dei processi di supporto, dei soggetti terzi e delle risorse informatiche individuate e classificate, nonché le loro interdipendenze, considerando come minimo i requisiti di riservatezza, integrità e disponibilità.
- L'analisi di impatto tiene conto delle caratteristiche di funzionamento dell'organizzazione e dei processi aziendali, in particolare considera:
    - Le specificità connesse con la localizzazione dei siti rilevanti;
    - I profili di concentrazione geografica;
    - La complessità dell'attività caratteristica del business e il grado di automazione raggiunto;
    - Le dimensioni aziendali e l'articolazione territoriale;
    - Il livello di esternalizzazione di funzioni aziendali rilevanti;
    - L'assetto organizzativo in termini di accentramento o decentramento dei processi critici;
    - I vincoli derivanti da interdipendenze, anche tra e con fornitori, clienti e altri operatori;
    - I rischi operativi e anche gli altri rischi (es. di mercato e di liquidità).
- Le Società del Conglomerato Finanziario 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 incidenti, con particolare attenzione ai processi che attengono alla gestione dei rapporti con la clientela e alla registrazione di fatti contabili;

- Il Piano di Continuità Operativa definisce i criteri di identificazione dei processi “critici” e ne documenta il periodico aggiornamento;
- 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 l’obiettivo di punto di ripristino e collabora attivamente alla realizzazione delle misure di continuità operativa;
- Il Piano di Continuità Operativa stabilisce i tempi di ripristino e gli obiettivi di punto 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 regole di conservazione di copie di documenti importanti in luoghi remoti rispetto ai documenti originali;
- Il piano di continuità operativa considera anche opzioni alternative nel caso in cui il ripristino non sia attuabile nel breve periodo a causa di costi, rischi, fattori logistici o circostanze impreviste;
- Il piano di continuità operativa definisce le modalità di comunicazione con la clientela, le controparti rilevanti, le autorità e i media;
- Il Piano di Continuità Operativa individua il personale essenziale per assicurare la continuità operativa dei processi critici e fornisce indicazioni 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;
- Le Società del Conglomerato Finanziario aggiornano periodicamente il Piano di Continuità Operativa. Nel caso di governo accentrato presso la Capogruppo il piano di quest’ultima documenta anche i processi e le procedure delle Controllate;

- Ciascuna Società prevede e pianifica verifiche di funzionamento dei processi critici
    - con frequenza e modalità coerente alla rilevanza dei rischi dei processi rilevati;
    - con 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 dell'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:
    - Laddove applicabile le verifiche prevedono l'attivazione dei collegamenti di rete presso il sito alternativo e l'esecuzione delle procedure di controllo della funzionalità e della prestazione dei siti alternativi;
    - I risultati delle prove sono documentati per iscritto e portati all'attenzione degli organi aziendali, delle unità operative coinvolte e alla funzione internal auditing;
    - a fronte di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive;
- Le Società del Conglomerato Finanziario comunicano tempestivamente alla Capogruppo eventuali incidenti e le conseguenti attivazioni di procedure di Continuità Operativa.
- Il Responsabile della Continuità Operativa della Capogruppo viene tempestivamente informato circa i referenti della Continuità Operativa delle Società Controllate (italiane ed estere), aggiornando la lista dei contatti utili in caso di crisi.

5.4 PRINCIPI DI BUSINESS CONTINUITY IN CASO DI RICORSO A SOGGETTI ESTERNI PER LA PRESTAZIONE DI SERVIZI ICT, ESTERNALIZZAZIONE, INFRASTRUTTURE E CONTROPARTI RILEVANTI

- In caso di ricorso a soggetti esterni per la prestazione di servizi ICT e di esternalizzazione di funzioni aziendali connesse allo svolgimento dei processi

critici, il Piano di Continuità Operativa prevede le misure da attuare in caso di crisi con impatto rilevante sull'operatore, sul soggetto terzo o sul fornitore dei servizi;

- Nel contratto di outsourcing (o nei relativi allegati) sono formalizzati i livelli di servizio assicurati in caso di crisi e le soluzioni di Continuità Operativa poste in atto dal soggetto terzo o dal fornitore di servizi esternalizzati, adeguati al conseguimento degli obiettivi aziendali e coerenti con le prescrizioni della Banca d'Italia. Sono altresì stabilite le modalità di partecipazione della società cliente, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori;
- Le Società del Conglomerato Finanziario acquisiscono i Piani di Continuità Operativa di soggetti terzi o dei fornitori di servizi critici esternalizzati o dispongono di informazioni adeguate al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità operativa realizzate all'interno;
- Tra le Società del Conglomerato Finanziario ed i soggetti terzi o i fornitori di servizi critici esternalizzati sono previsti flussi informativi tempestivi per la segnalazione di incidenti e la pronta attivazione delle procedure di Continuità Operativa;
- Per servizi essenziali dell'operatore le Società del Conglomerato Finanziario possono valutare il ricorso a fornitori alternativi in caso di emergenza;
- Il Responsabile della Continuità Operativa della Capogruppo viene tempestivamente informato circa i referenti della Continuità Operativa dei fornitori rilevanti, aggiornando la lista dei contatti utili in caso di crisi.

6. NORMATIVA DI RIFERIMENTO

I principali riferimenti normativi, regolamentari e di best practice in tema sono:

- EBA/CESB: Guidelines on Internal Governance
- Banca d'Italia – Circolare n. 285 del 17 dicembre 2013 – Disposizioni di Vigilanza per le Banche – Parte I, Titolo IV, Capitolo 5 "La continuità operativa" e successivi aggiornamenti
- Banca d'Italia – Circolare n.288 – Disposizioni di Vigilanza per gli Intermediari Finanziari
- IVASS – Regolamento n.38 del 3 luglio 2018
- Banca d'Italia – Provvedimento del 23 luglio 2019 – Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica
- Orientamenti in materia di esternalizzazioni emanati da EBA il 21 febbraio 2019 (EBA/GL/2019/02)
- Orientamenti EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (ICT) e di sicurezza del 28 novembre 2019 (EBA/GL/2019/04).
- Consob / Banca d'Italia – Regolamento congiunto in materia di organizzazione e procedure degli intermediari – 15 febbraio 2018
- Business Continuity Institute: Good Practice Guidelines 2018