S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

ATTO N. 27/MSP

ISTITUZIONE, ORGANIZZAZIONE E APPROVAZIONE DEL PIANO DI CONTINUITÀ OPERATIVA DEL MERCATO SOVRANO DEI POPOLI

Denominazione: Piano di Continuità Operativa del Mercato Sovrano dei Popoli – PCO-MSP.

Codice documentale: SIPSE/MSP/ATTO-27.

Ente emanante: Sistema delle Istituzioni dei Popoli per la Sovranità Economica – SIPSE.

Ambito di applicazione: Mercato Sovrano dei Popoli – MSP e strutture operative formalmente assoggettate.

Documento istitutivo di riferimento: Atto n. 25/MSP.

Regolamento attuativo di riferimento: Atto n. 26/MSP.

Riferimento metodologico principale: ISO 22301 – Business Continuity Management Systems.

PREAMBOLO

Il Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE),

considerato che la continuità delle funzioni istituzionali, amministrative, economiche, documentali e tecnologiche costituisce condizione essenziale per la stabilità organizzativa del Mercato Sovrano dei Popoli;

considerata la necessità di predisporre procedure preventive e organizzative idonee a fronteggiare eventi che possano compromettere la regolare esecuzione delle attività;

visto l'Atto n. 25/MSP, con il quale è stato istituito il Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli (SIGR-MSP);

visto l'Atto n. 26/MSP, recante il Regolamento operativo del SIGR-MSP;

ritenuto necessario definire un Piano di Continuità Operativa che identifichi le funzioni essenziali, le priorità di ripristino, le responsabilità, le risorse minime e le procedure di emergenza;

riconosciuta l'importanza della protezione delle registrazioni, della documentazione istituzionale, dei processi di gestione delle unità monetarie, delle garanzie e delle esposizioni;

considerata l'esigenza di garantire la continuità organizzativa anche in presenza di indisponibilità dei responsabili, delle infrastrutture o dei fornitori esterni;

assumendo come riferimento metodologico la norma ISO 22301, unitamente ai principi di gestione dei rischi della ISO 31000;

adotta il presente Atto.

TITOLO I – ISTITUZIONE E FINALITÀ DEL PCO-MSP

Articolo 1 – Istituzione

1. È istituito il Piano di Continuità Operativa del Mercato Sovrano dei Popoli, denominato PCO-MSP.
2. Il PCO-MSP costituisce lo strumento organizzativo e procedurale attraverso il quale il MSP definisce le modalità di mantenimento, gestione alternativa e ripristino delle proprie funzioni essenziali in presenza di eventi avversi.
3. Il Piano opera nell'ambito del SIGR-MSP e ne costituisce uno degli strumenti attuativi fondamentali.
4. Il PCO-MSP si applica alle strutture e alle attività formalmente ricomprese nell'organizzazione del Mercato Sovrano dei Popoli.
5. Il Piano è soggetto a revisione periodica e deve essere concretamente attuato mediante procedure, assegnazione delle responsabilità, disponibilità delle risorse e prove documentate.

Articolo 2 – Finalità

Il PCO-MSP persegue le seguenti finalità:

1. assicurare la continuità delle funzioni istituzionali essenziali;
2. limitare le conseguenze delle interruzioni operative;
3. mantenere la disponibilità delle informazioni necessarie;
4. proteggere i registri e la documentazione;
5. garantire la continuità delle procedure amministrative;
6. preservare l'integrità delle registrazioni;
7. individuare procedure alternative per le funzioni critiche;
8. ridurre la dipendenza da singoli soggetti e fornitori;
9. assicurare la sostituzione temporanea dei responsabili;
10. definire priorità e tempi obiettivo di ripristino;
11. coordinare le attività durante le emergenze;
12. consentire il ritorno controllato alle condizioni operative ordinarie.

Articolo 3 – Principi di continuità

Il PCO-MSP si fonda sui seguenti principi:

a. priorità delle funzioni essenziali;

b. protezione delle persone e delle informazioni;

c. prevenzione delle interruzioni;

d. proporzionalità delle misure;

e. separazione delle responsabilità;

f. disponibilità di procedure alternative;

g. conservazione delle evidenze;

h. tracciabilità delle decisioni;

i. verifica dell'effettiva capacità di ripristino;

j. miglioramento continuo.

Articolo 4 – Ambito funzionale

Il Piano comprende:

1. continuità istituzionale;
2. continuità amministrativa;
3. continuità documentale;
4. continuità dei registri;
5. continuità tecnologica;
6. continuità delle comunicazioni;
7. continuità dei controlli;
8. continuità dei processi di riconciliazione;
9. continuità delle procedure di gestione delle garanzie;
10. continuità delle attività di monitoraggio.

La continuità di una funzione non comporta automaticamente la possibilità di eseguire attività che richiedono autorizzazioni, disponibilità finanziarie o condizioni operative non presenti.

TITOLO II – ANALISI DI IMPATTO SULLE ATTIVITÀ

Articolo 5 – Business Impact Analysis

1. È istituita la Business Impact Analysis del MSP, denominata BIA-MSP.
2. La BIA-MSP identifica le conseguenze derivanti dall'interruzione delle attività e determina la priorità di mantenimento o ripristino.
3. L'analisi deve considerare:
   a. impatto istituzionale;
   b. impatto amministrativo;
   c. impatto economico;
   d. impatto tecnologico;
   e. impatto documentale;
   f. impatto giuridico;
   g. impatto sulla sicurezza;
   h. impatto sugli aderenti e sulle controparti interessate.
4. La BIA deve essere effettuata prima dell'attivazione definitiva delle funzioni essenziali e aggiornata in occasione di modifiche sostanziali.

Articolo 6 – Identificazione delle funzioni essenziali

Sono individuate, in via iniziale, le seguenti funzioni:

1. conservazione degli atti istituzionali;
2. gestione delle identità e delle autorizzazioni;
3. conservazione dei registri monetari;
4. conservazione del Registro Multilaterale delle Garanzie;
5. gestione delle registrazioni e riconciliazioni;
6. gestione delle informazioni relative alle esposizioni;
7. monitoraggio delle garanzie;
8. sicurezza delle infrastrutture;
9. comunicazioni istituzionali;
10. gestione degli incidenti;
11. controllo delle operazioni;
12. conservazione delle evidenze documentali.

L'inclusione nell'elenco non implica che tutte le funzioni siano già tecnicamente attive.

Articolo 7 – Classificazione delle funzioni

Le funzioni sono classificate in quattro categorie.

Classe F1 – Essenziale critica

Funzione la cui interruzione può compromettere la sicurezza, l'integrità dei registri o la capacità di governo del MSP.

Classe F2 – Essenziale prioritaria

Funzione necessaria per il mantenimento dei processi amministrativi e operativi fondamentali.

Classe F3 – Importante

Funzione il cui temporaneo arresto è gestibile mediante procedure alternative.

Classe F4 – Ordinaria

Funzione differibile senza compromissione immediata dell'organizzazione essenziale.

Articolo 8 – Valutazione dell'impatto temporale

La BIA considera l'evoluzione dell'impatto nel tempo.

Sono valutati:

1. impatto immediato;
2. impatto dopo quattro ore;
3. impatto dopo otto ore;
4. impatto dopo ventiquattro ore;
5. impatto dopo settantadue ore;
6. impatto dopo sette giorni.

Le soglie costituiscono intervalli di analisi e non autorizzano automaticamente l'interruzione o la prosecuzione di una determinata attività.

Articolo 9 – Dipendenze operative

Per ciascuna funzione essenziale devono essere individuate:

a. risorse umane;

b. applicazioni informatiche;

c. infrastrutture;

d. collegamenti di rete;

e. archivi;

f. documentazione;

g. fornitori;

h. eventuali intermediari;

i. autorizzazioni necessarie;

j. risorse economiche e materiali.

Ogni dipendenza deve essere registrata nel Registro delle Dipendenze Critiche (RDC-MSP).

TITOLO III – OBIETTIVI DI CONTINUITÀ E RIPRISTINO

Articolo 10 – Recovery Time Objective

1. Il Recovery Time Objective (RTO) rappresenta il tempo obiettivo massimo previsto per il ripristino di una funzione dopo un'interruzione.
2. Il valore RTO viene determinato attraverso la BIA.
3. Ogni funzione deve avere un obiettivo documentato, un responsabile e una procedura di ripristino.
4. L'RTO è un obiettivo di pianificazione e non una garanzia di prestazione già conseguita.

Articolo 11 – Recovery Point Objective

1. Il Recovery Point Objective (RPO) rappresenta il punto temporale di recupero dei dati e la quantità massima di perdita di informazioni che l'organizzazione intende tollerare.
2. L'RPO viene determinato in base alla criticità dei dati e alla frequenza di aggiornamento.
3. Devono essere definite procedure per verificare che le copie di sicurezza consentano effettivamente il recupero delle informazioni.

Articolo 12 – Obiettivi iniziali di continuità

Sono stabiliti i seguenti obiettivi progettuali iniziali:

Funzione	Classe	RTO obiettivo	RPO obiettivo
Identità e accessi	F1	8 ore	4 ore
Atti istituzionali	F1	8 ore	4 ore
RMUM	F1	8 ore	4 ore
RMG	F1	8 ore	4 ore
SMRC	F1	8 ore	2 ore
SIPSE Pay – componenti tecniche	F1	8 ore	2 ore
SMGCGE	F1	8 ore	4 ore
SMACG	F1	8 ore	4 ore
Comunicazioni istituzionali	F2	12 ore	8 ore
Archivi amministrativi	F2	24 ore	24 ore
Documentazione ordinaria	F3	48 ore	24 ore

1. Gli obiettivi sono subordinati alla valutazione tecnica delle infrastrutture effettivamente disponibili.
2. I valori devono essere confermati attraverso la BIA e le prove di ripristino.
3. Qualora un obiettivo non sia tecnicamente raggiungibile, il responsabile deve documentare la criticità e proporre misure alternative.
4. Nessuna funzione può essere dichiarata conforme agli obiettivi prima della verifica sperimentale.

Articolo 13 – Minimum Business Continuity Objective

1. È introdotto il Minimum Business Continuity Objective (MBCO).

2. Il MBCO definisce il livello minimo di attività che deve essere mantenuto durante un'interruzione.
3. Per ciascuna funzione devono essere definiti:
   a. attività indispensabili;
   b. attività temporaneamente sospendibili;
   c. risorse minime;
   d. personale necessario;
   e. strumenti alternativi;
   f. condizioni di riattivazione.
4. Il MBCO non deve comportare l'esecuzione di operazioni prive delle necessarie verifiche o autorizzazioni.

TITOLO IV – ORGANIZZAZIONE DELLA CONTINUITÀ

Articolo 14 – Comitato di Continuità Operativa

1. È istituito il Comitato di Continuità Operativa del MSP (CCO-MSP).
2. Il Comitato coordina la gestione organizzativa delle emergenze.
3. È composto da:
   a. rappresentante della Direzione MSP;
   b. responsabile UGR-MSP;
   c. responsabile UCV-MSP, con funzioni di verifica;
   d. responsabile tecnologico;
   e. responsabile della continuità operativa;
   f. responsabili delle funzioni interessate.
4. I componenti sono nominati con atto formale.
5. Le funzioni possono essere accorpate soltanto con adeguate salvaguardie e senza compromettere l'indipendenza dei controlli.

Articolo 15 – Responsabile della Continuità Operativa

Il Responsabile della Continuità Operativa (RCO-MSP):

1. mantiene aggiornato il PCO;
2. coordina le attività preparatorie;
3. verifica la disponibilità delle procedure;
4. coordina le simulazioni;
5. mantiene i contatti con i responsabili;
6. supporta il CCO-MSP;
7. predispone i rapporti sugli eventi;
8. verifica le attività di ripristino.

Articolo 16 – Responsabili delle funzioni essenziali

Ogni funzione essenziale deve avere:

1. un responsabile titolare;
2. un sostituto formalmente individuato;
3. una procedura alternativa;
4. un elenco delle risorse;
5. un elenco delle dipendenze;
6. una procedura di comunicazione;
7. un piano di ripristino.

Il responsabile deve mantenere aggiornate le informazioni relative alla propria funzione.

Articolo 17 – Sostituzione organizzativa

1. In caso di indisponibilità di un responsabile si attiva la procedura di sostituzione.
2. Il sostituto esercita esclusivamente le competenze formalmente delegate.
3. La sostituzione deve essere registrata con:
   a. nominativo del titolare;
   b. nominativo del sostituto;
   c. motivo;
   d. data di attivazione;
   e. ambito delle competenze;
   f. durata;
   g. data di cessazione.
4. Le funzioni di controllo indipendente non possono essere assorbite automaticamente dalle funzioni operative.

TITOLO V – SCENARI DI EMERGENZA

Articolo 18 – Scenari contemplati

Il PCO-MSP disciplina almeno i seguenti scenari:

1. indisponibilità dei sistemi informatici;
2. interruzione della connettività;
3. guasto delle infrastrutture;
4. perdita o corruzione dei dati;
5. attacco informatico;
6. compromissione delle credenziali;
7. indisponibilità dei responsabili;
8. indisponibilità dei locali;
9. interruzione dei servizi dei fornitori;
10. indisponibilità di servizi esterni essenziali;
11. perdita di documentazione;
12. eventi naturali o calamità;
13. interruzioni prolungate delle comunicazioni;
14. compromissione dell'integrità dei registri.

Articolo 19 – Emergenza informatica

In caso di compromissione informatica:

1. il responsabile tecnico valuta l'evento;
2. vengono isolati i sistemi compromessi, quando necessario;
3. sono protette le credenziali e le chiavi;
4. vengono preservate le evidenze;
5. viene informata la Direzione MSP;
6. l'UGR-MSP classifica il rischio;
7. viene valutata l'attivazione del PCO;
8. il ripristino viene effettuato attraverso procedure controllate.

Non è consentito riattivare un sistema compromesso senza una verifica adeguata della sua integrità e sicurezza.

Articolo 20 – Emergenza documentale

In caso di indisponibilità o perdita degli archivi:

1. viene verificata la disponibilità delle copie di sicurezza;
2. viene identificata l'ultima versione verificata;
3. viene ricostruita la cronologia delle modifiche;
4. vengono individuati eventuali documenti mancanti;
5. viene predisposto un verbale;
6. viene effettuato il recupero;
7. viene verificata la completezza documentale.

Articolo 21 – Emergenza istituzionale

In caso di indisponibilità di un organo o responsabile:

1. viene verificata la disciplina delle sostituzioni;
2. viene attivato il sostituto autorizzato;
3. sono mantenute le sole funzioni di competenza;
4. vengono sospese le decisioni che richiedono poteri non trasferibili;
5. viene mantenuta la tracciabilità delle deliberazioni.

Articolo 22 – Emergenza relativa ai fornitori

1. In caso di indisponibilità di un fornitore essenziale viene attivata la procedura alternativa prevista.
2. Il responsabile verifica:
   a. natura dell'interruzione;
   b. durata stimata;
   c. impatto sulle funzioni;
   d. disponibilità di soluzioni alternative;
   e. possibilità di migrazione;
   f. eventuali obblighi contrattuali.
3. In assenza di alternative affidabili, le attività dipendenti vengono sospese o limitate secondo la valutazione del rischio.

TITOLO VI – ATTIVAZIONE E GESTIONE DEL PCO

Articolo 23 – Condizioni di attivazione

Il PCO-MSP può essere attivato quando:

1. una funzione essenziale risulta indisponibile;
2. l'interruzione supera o rischia di superare il relativo RTO;
3. l'integrità delle informazioni è compromessa;
4. un evento minaccia la continuità istituzionale;
5. un fornitore essenziale non è disponibile;
6. un incidente informatico compromette l'operatività;
7. le procedure ordinarie non sono più sufficienti.

Articolo 24 – Procedura di attivazione

L'attivazione segue il procedimento:

Fase 1 – Rilevazione

Identificazione dell'evento.

Fase 2 – Segnalazione

Comunicazione al responsabile della funzione e alla Direzione MSP.

Fase 3 – Valutazione

Analisi dell'impatto e delle funzioni coinvolte.

Fase 4 – Decisione

Attivazione del PCO da parte del soggetto competente.

Fase 5 – Mobilitazione

Attivazione del CCO-MSP e dei responsabili interessati.

Fase 6 – Continuità

Attivazione delle procedure alternative.

Fase 7 – Ripristino

Recupero delle funzioni secondo le priorità.

Fase 8 – Verifica

Controllo della sicurezza, integrità e regolarità delle attività.

Fase 9 – Chiusura

Rientro documentato nella gestione ordinaria.

Articolo 25 – Verbale di attivazione

Ogni attivazione deve essere accompagnata da un verbale contenente:

1. identificativo dell'evento;
2. data e ora;
3. soggetto segnalante;
4. funzione interessata;
5. natura dell'interruzione;
6. impatto;
7. livello di criticità;
8. soggetto autorizzante;
9. misure adottate;
10. responsabili;
11. obiettivi di ripristino;
12. comunicazioni effettuate.

Articolo 26 – Modalità operative alternative

Durante l'emergenza possono essere utilizzate procedure alternative, purché:

a. formalmente autorizzate;

b. limitate alle funzioni necessarie;

c. tracciabili;

d. verificabili;

e. coerenti con la normativa applicabile;

f. reversibili;

g. sottoposte a riconciliazione successiva.

Le procedure alternative non possono derogare agli obblighi legali, ai requisiti autorizzativi o ai controlli indispensabili per la sicurezza delle operazioni.

TITOLO VII – CONTINUITÀ DEI SISTEMI E DEI REGISTRI

Articolo 27 – Registro Multilaterale delle Unità Monetarie

In caso di indisponibilità del RMUM:

1. viene sospesa la possibilità di effettuare modifiche non verificabili;
2. viene mantenuta una copia dell'ultima versione verificata;
3. le richieste ricevute possono essere registrate in un elenco temporaneo;
4. ogni richiesta riceve un identificativo provvisorio;
5. la registrazione definitiva avviene dopo il ripristino e la verifica;
6. viene effettuata una riconciliazione delle richieste pendenti.

La conservazione del registro non equivale all'effettiva disponibilità o convertibilità delle unità monetarie.

Articolo 28 – Registro Multilaterale delle Garanzie

In caso di indisponibilità del RMG:

1. viene preservata l'ultima copia verificata;
2. sono sospese le nuove attribuzioni non verificabili;
3. le garanzie già registrate mantengono il proprio stato documentale precedente;
4. non sono ammesse duplicazioni;
5. le richieste pendenti vengono annotate;
6. il ripristino è seguito da una verifica della cronologia.

Articolo 29 – SMGCGE e SMACG

In caso di indisponibilità dei sistemi di monitoraggio:

1. viene conservata l'ultima situazione verificata;
2. viene segnalata la mancata disponibilità dei dati aggiornati;
3. le elaborazioni non verificabili sono contrassegnate come provvisorie;
4. vengono sospese le decisioni che richiedono dati aggiornati non disponibili;
5. al ripristino viene eseguita la riconciliazione.

È vietato presentare dati non aggiornati come se fossero in tempo reale.

Articolo 30 – SMRC e SIPSE Pay

1. In caso di indisponibilità dei sistemi SMRC o delle componenti tecniche di SIPSE Pay, le attività interessate vengono gestite secondo le procedure di sicurezza e continuità approvate.
2. Le istruzioni non confermate devono mantenere lo stato di non eseguite o non regolate.
3. Non possono essere create duplicazioni attraverso l'inserimento manuale di operazioni già ricevute o elaborate.
4. Il ripristino deve prevedere:
   a. verifica delle operazioni;
   b. riconciliazione;
   c. individuazione delle duplicazioni;

d. controllo degli stati;
e. approvazione delle eventuali rettifiche.

5. Restano fermi i requisiti e le autorizzazioni eventualmente necessari per le attività di pagamento e regolamento.

TITOLO VIII – COMUNICAZIONI DI EMERGENZA

Articolo 31 – Sistema di comunicazione

Il MSP deve predisporre almeno due modalità indipendenti di comunicazione per le emergenze.

Le modalità possono comprendere:

1. posta elettronica istituzionale;
2. canale alternativo protetto;
3. comunicazione telefonica;
4. piattaforma documentale alternativa;
5. comunicazione formale tramite i responsabili designati.

La disponibilità effettiva dei canali deve essere verificata periodicamente.

Articolo 32 – Catena di comunicazione

La catena di comunicazione segue il seguente ordine:

1. responsabile della funzione interessata;
2. Responsabile della Continuità Operativa;
3. Direzione MSP;
4. UGR-MSP;
5. CCO-MSP;
6. Direttivo SIPSE, per gli eventi di competenza.

L'UCV-MSP riceve le informazioni necessarie per lo svolgimento delle verifiche indipendenti.

Articolo 33 – Comunicazioni esterne

1. Le comunicazioni verso aderenti, fornitori e soggetti interessati sono autorizzate dalla struttura competente.
2. Le informazioni devono essere accurate e proporzionate.
3. Devono essere distinti:
   a. evento rilevato;
   b. evento confermato;
   c. impatto verificato;
   d. misure adottate;
   e. tempi stimati;
   f. informazioni ancora da accertare.

4. Le comunicazioni previste dalla legge o dai contratti devono rispettare i relativi termini e requisiti.

TITOLO IX – TEST E VERIFICHE

Articolo 34 – Programma di test

Il PCO-MSP è sottoposto a verifiche periodiche mediante:

1. simulazioni documentali;
2. esercitazioni dei responsabili;
3. test di indisponibilità;
4. prove di comunicazione;
5. simulazioni di indisponibilità dei fornitori;
6. prove di recupero documentale;
7. prove di attivazione delle procedure alternative;
8. esercitazioni di continuità istituzionale.

Articolo 35 – Frequenza

Sono previste le seguenti frequenze minime:

Attività	Frequenza
Revisione dei contatti	Trimestrale
Verifica delle procedure	Trimestrale
Test delle comunicazioni	Semestrale
Esercitazione dei responsabili	Semestrale
Simulazione di emergenza	Semestrale
Verifica complessiva del PCO	Annuale
Revisione dopo incidente critico	Straordinaria

Articolo 36 – Rapporto di prova

Ogni test deve produrre un rapporto contenente:

1. scenario;
2. obiettivi;
3. partecipanti;
4. procedure utilizzate;
5. tempi misurati;
6. risultati;
7. anomalie;
8. criticità;
9. azioni correttive;
10. responsabile;
11. termine di completamento;

12. verifica conclusiva.

Articolo 37 – Mancato superamento delle prove

1. Se una prova evidenzia il mancato raggiungimento degli obiettivi, la funzione interessata viene classificata secondo il livello di rischio effettivo.
2. L'UGR-MSP predispone un piano correttivo.
3. Il responsabile della funzione attua le misure.
4. L'UCV-MSP verifica l'effettiva risoluzione.
5. La funzione non può essere dichiarata pienamente conforme agli obiettivi di continuità fino alla conclusione positiva delle verifiche necessarie.

TITOLO X – DOCUMENTAZIONE E REGISTRAZIONE

Articolo 38 – Registri del PCO-MSP

Sono istituiti i seguenti strumenti:

1. BIA-MSP – Registro delle Analisi di Impatto;
2. RFO-MSP – Registro delle Funzioni Operative;
3. RCO-MSP – Registro dei Responsabili della Continuità;
4. RPE-MSP – Registro delle Procedure di Emergenza;
5. RPC-MSP – Registro delle Prove di Continuità;
6. RAE-MSP – Registro delle Attivazioni di Emergenza;
7. RDC-MSP – Registro delle Dipendenze Critiche.

Gli strumenti già istituiti dall'Atto 25 e dall'Atto 26 sono utilizzati in modo coordinato, evitando duplicazioni documentali.

Articolo 39 – Conservazione delle evidenze

1. Tutte le attivazioni, le comunicazioni, le decisioni e le prove devono essere conservate.
2. La documentazione deve riportare data, versione e responsabile.
3. Le rettifiche devono mantenere la cronologia delle modifiche.
4. Gli archivi devono essere protetti da accessi non autorizzati e perdita di integrità.

TITOLO XI – GOVERNANCE, REVISIONE E LIMITI

Articolo 40 – Supervisione

Il Direttivo SIPSE esercita la supervisione istituzionale sul PCO-MSP attraverso:

1. approvazione degli indirizzi;

2. esame delle relazioni;
3. valutazione delle criticità;
4. verifica delle misure correttive;
5. approvazione delle revisioni sostanziali.

Articolo 41 – Relazione annuale

Il Responsabile della Continuità Operativa predispone una relazione annuale contenente:

a. stato di attuazione del Piano;

b. funzioni censite;

c. risultati della BIA;

d. obiettivi RTO e RPO;

e. risultati delle esercitazioni;

f. criticità rilevate;

g. dipendenze esterne;

h. stato delle misure correttive;

i. proposte di miglioramento.

Articolo 42 – Revisione straordinaria

Il Piano è sottoposto a revisione straordinaria in caso di:

1. modifiche sostanziali dell'organizzazione;
2. introduzione di nuove funzioni essenziali;
3. cambiamenti tecnologici rilevanti;
4. incidenti critici;
5. indisponibilità prolungata;
6. variazioni dei fornitori;
7. modifiche normative;
8. mancato superamento delle prove.

Articolo 43 – Limiti di applicazione

1. Il PCO-MSP costituisce uno strumento interno di continuità organizzativa.
2. La sua approvazione non dimostra automaticamente la disponibilità delle infrastrutture, dei finanziamenti, dei servizi esterni o delle risorse necessarie.
3. Il Piano non attribuisce autorizzazioni bancarie, finanziarie o di pagamento.
4. Non costituisce garanzia di continuità assoluta o di assenza di perdite.
5. Le attività soggette a requisiti normativi o autorizzativi devono essere svolte nel rispetto della legislazione applicabile.

TITOLO XII – DISPOSIZIONI FINALI

Articolo 44 – Documenti attuativi

Per l'effettiva applicazione del presente Atto sono predisposti:

1. Manuale operativo PCO-MSP;
2. Modello BIA-MSP;
3. Elenco delle funzioni essenziali;
4. Matrice delle responsabilità;
5. Procedura di attivazione delle emergenze;
6. Piano delle comunicazioni;
7. Schede degli scenari di emergenza;
8. Modello di verbale di attivazione;
9. Modello di rapporto di esercitazione;
10. Piano annuale di verifica.

Articolo 45 – Attuazione progressiva

L'attuazione del PCO-MSP si articola in sette fasi:

Fase I – Censimento: identificazione delle funzioni.

Fase II – Analisi: completamento della BIA.

Fase III – Organizzazione: nomina dei responsabili e dei sostituti.

Fase IV – Pianificazione: definizione delle procedure alternative.

Fase V – Preparazione: predisposizione delle risorse e delle infrastrutture.

Fase VI – Verifica: esercitazioni e prove.

Fase VII – Validazione interna: verifica documentale e autorizzazione delle procedure operative.

L'effettiva attivazione è attestata esclusivamente sulla base delle verifiche eseguite e delle evidenze conservate.

Articolo 46 – Entrata in vigore

Il presente Atto entra in vigore dalla data della sua formale approvazione da parte dell'organo competente del SIPSE.

Articolo 47 – Clausola di revisione

Il presente Atto è sottoposto a revisione almeno annuale e comunque ogniqualvolta intervengano modifiche sostanziali dell'organizzazione o delle condizioni operative del MSP.

DISPOSIZIONE CONCLUSIVA

Con l'Atto n. 27/MSP il Sistema delle Istituzioni dei Popoli per la Sovranità Economica istituisce il Piano di Continuità Operativa del Mercato Sovrano dei Popoli, definendo un quadro organizzativo volto a preservare le funzioni essenziali anche in condizioni di emergenza.

La continuità viene riconosciuta come responsabilità permanente dell'organizzazione e non come semplice risposta occasionale a un evento avverso.

Il MSP deve poter identificare le proprie funzioni fondamentali, conoscere le proprie dipendenze, disporre di procedure alternative, assegnare responsabilità precise e dimostrare attraverso prove documentate la propria capacità di mantenere o ripristinare le attività.

La continuità istituzionale si costruisce prima dell'emergenza, attraverso responsabilità definite, risorse disponibili e procedure verificabili.

S.I.P.S.E. – Sistema delle Istituzioni dei Popoli per la Sovranità Economica

MERCATO SOVRANO DEI POPOLI – MSP

Atto n. 27/MSP

Codice documentale: SIPSE/MSP/ATTO-27

Data di approvazione: da determinare.

Organo approvante: _____

Responsabile della conservazione documentale: _____