S.I.P.S.E. – SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

ATTO N. 25/MSP

SISTEMA DI GESTIONE DEI RISCHI, DELLA CONTINUITÀ OPERATIVA E DELLA RESILIENZA ISTITUZIONALE

MERCATO SOVRANO DEI POPOLI

DOCUMENTO ISTITUTIVO

CODICE DOCUMENTALE

SIPSE/MSP/ATTO-25

AMBITO

Governance e resilienza

APPLICAZIONE

Sistema interno MSP

STATO

Istituzione e disciplina

TESTO NORMATIVO COMPLETO

S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

ATTO N. 25/MSP

ISTITUZIONE DEL SISTEMA DI GESTIONE DEI RISCHI, DELLA CONTINUITÀ OPERATIVA E DELLA

RESILIENZA ISTITUZIONALE DEL MERCATO SOVRANO DEI POPOLI

Titolo ufficiale: Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli – SIGR-MSP.

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

Ambito istituzionale: Mercato Sovrano dei Popoli – MSP.

Riferimento organizzativo: Assemblea Generale dei Popoli, Direttivo SIPSE, Direzione MSP e unità operative e di controllo competenti.

PREAMBOLO

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

considerata la necessità di assicurare al Mercato Sovrano dei Popoli un'organizzazione stabile, verificabile, prudente e capace di affrontare situazioni di rischio, interruzione, indisponibilità o compromissione delle proprie attività;

considerato che lo sviluppo di un sistema economico multilaterale richiede strumenti permanenti di prevenzione, identificazione, valutazione, contenimento e monitoraggio dei rischi;

riconosciuta l'importanza della continuità delle funzioni istituzionali, amministrative, documentali, tecnologiche, contabili e operative;

ritenuto necessario distinguere le responsabilità di gestione, autorizzazione, controllo, verifica e supervisione;

tenuto conto degli atti precedentemente adottati nell'ambito del MSP, con particolare riferimento al Sistema di Monitoraggio delle Garanzie e della Copertura delle Esposizioni (SMGCGE), al Registro Multilaterale delle Garanzie (RMG), al Sistema di Monitoraggio e Allerta delle Coperture e delle Garanzie (SMACG) e ai relativi manuali tecnici;

assumendo quali riferimenti metodologici, nei rispettivi ambiti di applicabilità:

- ISO 31000 – Risk Management;
- ISO 22301 – Business Continuity Management Systems;
- ISO/IEC 27001 – Information Security Management Systems;
- ISO/IEC 27005 – Information Security Risk Management;
- principi di controllo interno, audit, segregazione delle funzioni e gestione degli incidenti;
- principi internazionali di resilienza operativa applicabili alle infrastrutture e ai servizi finanziari;

adotta il presente Atto.

TITOLO I – DISPOSIZIONI GENERALI

Articolo 1 – Istituzione del sistema

1. È istituito il Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli, denominato SIGR-MSP.
2. Il SIGR-MSP costituisce l'architettura organizzativa, metodologica, documentale e operativa attraverso la quale il MSP identifica, valuta, tratta, controlla e monitora i rischi connessi alle proprie attività.
3. Il sistema comprende:
   a. gestione integrata dei rischi;
   b. controllo preventivo e successivo;
   c. continuità operativa;
   d. sicurezza delle informazioni;
   e. protezione delle infrastrutture tecnologiche;
   f. gestione degli incidenti;
   g. recupero e ripristino delle funzioni;
   h. resilienza istituzionale;
   i. verifica periodica dell'efficacia dei controlli.
4. Il SIGR-MSP opera secondo criteri di proporzionalità, prudenza, tracciabilità, responsabilità e verificabilità.

Articolo 2 – Finalità

Il sistema persegue le seguenti finalità:

1. prevenire situazioni che possano compromettere il funzionamento del MSP;
2. ridurre la probabilità e l'impatto degli eventi avversi;
3. proteggere l'integrità delle registrazioni e dei documenti;
4. preservare la disponibilità dei servizi istituzionali e tecnologici;
5. tutelare le informazioni e i dati trattati;
6. individuare tempestivamente anomalie e irregolarità;
7. limitare gli effetti di interruzioni operative;
8. assicurare il ripristino ordinato delle funzioni essenziali;
9. proteggere la continuità delle procedure di controllo delle garanzie e delle esposizioni;
10. mantenere la fiducia organizzativa attraverso procedure trasparenti e verificabili.

Articolo 3 – Ambito di applicazione

1. Il SIGR-MSP si applica alle strutture e alle attività interne del Mercato Sovrano dei Popoli.
2. Sono interessati:
   a. Direzione MSP;
   b. Direzione SMRC;
   c. SIPSE Pay;
   d. Unità di Valorizzazione;
   e. Unità di Gestione dei Rischi;
   f. Unità di Controllo e Verifica;
   g. Registro Multilaterale delle Unità Monetarie (RMUM);

h. Registro Multilaterale delle Garanzie (RMG);
i. Sistema di Monitoraggio delle Garanzie e della Copertura delle Esposizioni (SMGCGE);
j. Sistema di Monitoraggio e Allerta delle Coperture e delle Garanzie (SMACG);
k. infrastrutture informatiche e documentali;
l. soggetti operativi formalmente ammessi al sistema, nei limiti degli obblighi assunti.

3. L'applicazione a soggetti esterni richiede un titolo documentale, contrattuale o regolamentare appropriato.
4. Il presente Atto non attribuisce al MSP poteri di vigilanza pubblicistica, autorizzazione finanziaria o controllo su soggetti terzi.

Articolo 4 – Principi fondamentali

Il SIGR-MSP opera sulla base dei seguenti principi:

1. prevenzione prima dell'intervento correttivo;
2. proporzionalità del controllo rispetto al rischio;
3. separazione tra gestione e verifica;
4. indipendenza delle valutazioni;
5. documentazione delle decisioni;
6. identificazione univoca degli eventi;
7. divieto di duplicazione delle garanzie e delle coperture;
8. prudenza nella valutazione delle disponibilità;
9. trasparenza delle procedure;
10. riservatezza delle informazioni;
11. continuità delle funzioni essenziali;
12. miglioramento continuo.

TITOLO II – CLASSIFICAZIONE DEI RISCHI

Articolo 5 – Tassonomia dei rischi

Il MSP adotta una classificazione integrata dei rischi, articolata nelle seguenti categorie.

5.1 Rischio istituzionale

Comprende:

- conflitti di competenza;
- interruzione degli organi decisionali;
- perdita di documentazione istituzionale;
- mancata esecuzione delle deliberazioni;
- concentrazione eccessiva delle responsabilità;
- assenza di sostituzioni organizzative.

5.2 Rischio operativo

Comprende:

- errori procedurali;
- mancata esecuzione delle attività;
- duplicazione delle operazioni;
- registrazioni incomplete;
- ritardi amministrativi;
- indisponibilità del personale;
- errori di riconciliazione.

5.3 Rischio finanziario e di liquidità

Comprende:

- insufficienza delle disponibilità;
- disallineamento temporale delle entrate e delle uscite;
- esposizioni non adeguatamente coperte;
- concentrazione delle disponibilità;
- ritardi di regolamento;
- mancata esecuzione degli obblighi;
- rischio di controparte.

La rilevazione interna di tali rischi non equivale a una certificazione di solvibilità o liquidità.

5.4 Rischio monetario e di cambio

Comprende:

- oscillazione dei valori di riferimento;
- divergenza tra valore contabile e valore realizzabile;
- rischio di conversione;
- disallineamento tra unità di conto;
- indisponibilità di strumenti di conversione;
- rischio di concentrazione monetaria.

La parità progettuale di riferimento dello ZEC, ove utilizzata, non costituisce garanzia automatica di convertibilità, rimborso o disponibilità di euro.

5.5 Rischio relativo alle garanzie

Comprende:

- inesistenza o insufficienza documentale;
- perdita di valore;
- indisponibilità;
- doppia attribuzione;
- mancata perfezione giuridica;
- impossibilità di escussione;
- variazione delle condizioni di efficacia.

Le garanzie sono considerate esclusivamente secondo il rispettivo stato documentale, giuridico e operativo.

5.6 Rischio tecnologico e informatico

Comprende:

- guasti hardware;
- malfunzionamenti software;
- indisponibilità dei server;
- perdita o corruzione dei dati;
- errori di aggiornamento;
- incompatibilità tra sistemi;
- interruzione delle comunicazioni;
- vulnerabilità infrastrutturali.

5.7 Rischio informatico e di sicurezza

Comprende:

- accessi non autorizzati;
- furto di credenziali;
- compromissione di account;
- attacchi informatici;
- malware;
- ransomware;
- esfiltrazione di informazioni;
- alterazione delle registrazioni;
- compromissione delle chiavi crittografiche.

5.8 Rischio di frode e abuso

Comprende:

- falsificazione documentale;
- alterazione dei dati;
- uso improprio delle credenziali;
- dichiarazioni non veritiere;
- appropriazione indebita;
- conflitti di interesse non dichiarati;
- manipolazione delle procedure;
- tentativi di doppio utilizzo delle coperture.

5.9 Rischio giuridico e regolamentare

Comprende:

- inosservanza della normativa applicabile;
- inadeguatezza contrattuale;
- insufficienza delle autorizzazioni;

- controversie;
- incertezza sulla titolarità dei diritti;
- mancata conformità agli obblighi di protezione dei dati;
- esercizio di attività riservate senza titolo.

5.10 Rischio di controparte e concentrazione

Comprende:

- dipendenza da un singolo operatore;
- dipendenza da un singolo fornitore tecnologico;
- concentrazione delle disponibilità;
- dipendenza da infrastrutture esterne;
- incapacità della controparte di adempiere;
- indisponibilità di servizi essenziali.

5.11 Rischio reputazionale e informativo

Comprende:

- comunicazioni inesatte;
- divulgazione di informazioni riservate;
- dichiarazioni non documentate;
- rappresentazioni improprie delle capacità del MSP;
- perdita di fiducia degli aderenti.

Articolo 6 – Identificazione e registrazione

1. Ogni rischio individuato deve essere registrato nell'Anagrafe Interna dei Rischi del MSP.
2. Ogni registrazione contiene:
   a. identificativo univoco;
   b. categoria;
   c. descrizione;
   d. origine;
   e. probabilità stimata;
   f. impatto potenziale;
   g. livello di rischio;
   h. responsabile;
   i. misure di mitigazione;
   j. scadenza della revisione;
   k. stato di trattamento;
   l. evidenze documentali.
3. Il codice identificativo assume la seguente struttura:

MSP-RISK-ANNO-NUMERO

4. Ogni modifica deve essere tracciata, datata e attribuita al soggetto responsabile.

TITOLO III – VALUTAZIONE E TRATTAMENTO DEI RISCHI

Articolo 7 – Metodo di valutazione

1. Il rischio è valutato considerando probabilità e impatto.
2. Il sistema utilizza una scala da 1 a 5 per entrambe le dimensioni.

Indice di rischio inerente:

$R = P \times I$

Dove:

- R = indice di rischio;
- P = probabilità;
- I = impatto.

3. La classificazione è la seguente:

Punteggio	Livello	Qualificazione
1–4	Basso	Controllo ordinario
5–9	Moderato	Monitoraggio periodico
10–15	Elevato	Mitigazione prioritaria
16–25	Critico	Intervento immediato

4. Il punteggio non costituisce una probabilità matematica di perdita, ma uno strumento interno di classificazione e priorità.

Articolo 8 – Rischio residuo

1. Dopo l'applicazione delle misure di mitigazione viene determinato il rischio residuo.
2. La valutazione deve considerare:
   a. efficacia dei controlli;
   b. adeguatezza delle procedure;
   c. indipendenza delle verifiche;
   d. disponibilità delle risorse;
   e. dipendenze esterne;
   f. evidenze degli incidenti precedenti.
3. Un rischio critico non può essere considerato accettabile sulla sola base di una dichiarazione del responsabile operativo.
4. L'accettazione di rischi elevati richiede motivazione scritta, individuazione delle responsabilità e approvazione dell'organo competente.

Articolo 9 – Piano di trattamento

Per ogni rischio elevato o critico deve essere predisposto un piano di trattamento contenente:

1. descrizione del problema;
2. obiettivo di mitigazione;
3. misure preventive;
4. misure correttive;
5. responsabile dell'attuazione;
6. risorse necessarie;
7. termine di completamento;
8. indicatori di efficacia;
9. procedura di verifica;
10. eventuale piano alternativo.

Le strategie ammesse sono:

- evitare il rischio;
- ridurre la probabilità;
- ridurre l'impatto;
- trasferire contrattualmente una parte del rischio, ove legittimo;
- accettare il rischio residuo entro limiti formalmente approvati.

TITOLO IV – GOVERNANCE E RESPONSABILITÀ

Articolo 10 – Direzione del sistema

1. La responsabilità istituzionale del SIGR-MSP compete al Direttivo SIPSE, nei limiti delle competenze attribuite dagli atti organizzativi.
2. Il Direttivo:
   a. approva gli indirizzi generali;
   b. definisce la propensione al rischio;
   c. approva le soglie di tolleranza;
   d. riceve le relazioni periodiche;
   e. dispone gli interventi straordinari;
   f. verifica l'attuazione delle misure correttive.

Articolo 11 – Unità di Gestione dei Rischi

1. È istituita l'Unità di Gestione dei Rischi del MSP (UGR-MSP).
2. L'UGR-MSP svolge funzioni di:
   a. identificazione dei rischi;
   b. valutazione;
   c. classificazione;
   d. aggiornamento del registro;
   e. predisposizione dei piani di mitigazione;
   f. monitoraggio degli indicatori;
   g. coordinamento delle procedure di continuità;
   h. predisposizione delle relazioni.

3. L'UGR-MSP non può certificare autonomamente la correttezza delle attività che essa stessa ha eseguito.

Articolo 12 – Unità di Controllo e Verifica

1. È istituita l'Unità di Controllo e Verifica (UCV-MSP).
2. Essa verifica:
   a. completezza delle registrazioni;
   b. corretta applicazione delle procedure;
   c. segregazione delle funzioni;
   d. adeguatezza delle evidenze;
   e. efficacia delle misure di mitigazione;
   f. gestione degli incidenti;
   g. rispetto delle procedure di continuità.
3. L'UCV-MSP deve operare con autonomia funzionale rispetto alle unità sottoposte a verifica.
4. Le anomalie sono riportate in un verbale documentale.

Articolo 13 – Responsabilità operative

Ogni struttura del MSP è responsabile dei rischi direttamente connessi alle proprie attività.

In particolare:

- Direzione MSP: coordinamento generale;
- Direzione SMRC: rischi di registrazione, compensazione e riconciliazione;
- SIPSE Pay: rischi relativi alle funzioni tecniche e ai processi di pagamento eventualmente autorizzati;
- Unità di Valorizzazione: rischi di valutazione;
- UGR-MSP: coordinamento e monitoraggio dei rischi;
- UCV-MSP: verifica indipendente;
- responsabili tecnologici: sicurezza e disponibilità delle infrastrutture.

La ripartizione non esonera ciascun soggetto dagli obblighi previsti dalla normativa applicabile.

Articolo 14 – Separazione delle funzioni

1. Nessun soggetto può concentrare senza adeguate salvaguardie la facoltà di:
   a. creare una registrazione;
   b. autorizzarla;
   c. modificarla;
   d. verificarne la correttezza;
   e. dichiararla definitivamente validata.
2. Le operazioni critiche devono prevedere un controllo indipendente o un principio di doppia approvazione.
3. Le credenziali amministrative devono essere individuali, nominative e revocabili.

TITOLO V – CONTINUITÀ OPERATIVA

Articolo 15 – Istituzione del Piano di Continuità Operativa

1. È istituito il Piano di Continuità Operativa del Mercato Sovrano dei Popoli (PCO-MSP).
2. Il piano definisce le procedure necessarie per mantenere o ripristinare le funzioni essenziali in presenza di:
   a. guasti;
   b. interruzioni;
   c. indisponibilità delle infrastrutture;
   d. incidenti informatici;
   e. eventi naturali;
   f. indisponibilità del personale;
   g. perdita di documentazione;
   h. indisponibilità di fornitori;
   i. compromissione di sistemi o credenziali.
3. Il PCO-MSP deve essere aggiornato in funzione dell'evoluzione delle attività.

Articolo 16 – Analisi di impatto sulle attività

1. È introdotta la Business Impact Analysis (BIA).
2. La BIA individua:
   a. funzioni essenziali;
   b. dipendenze tecnologiche;
   c. dipendenze organizzative;
   d. dipendenze da fornitori;
   e. conseguenze dell'interruzione;
   f. risorse necessarie al ripristino;
   g. priorità operative.
3. Ogni funzione deve essere classificata secondo il livello di criticità.
4. La BIA deve essere aggiornata almeno annualmente e in occasione di modifiche sostanziali.

Articolo 17 – Obiettivi di ripristino

1. Il MSP adotta due indicatori fondamentali:

RTO – Recovery Time Objective

Tempo massimo obiettivo entro il quale una funzione deve essere ripristinata.

RPO – Recovery Point Objective

Intervallo massimo obiettivo di perdita dei dati espresso in termini temporali.

2. Gli obiettivi iniziali di pianificazione sono:

Funzione	RTO obiettivo	RPO obiettivo
Identità e accessi	8 ore	4 ore
Registri istituzionali	8 ore	4 ore
RMUM	8 ore	4 ore

RMG	8 ore	4 ore
SMRC	8 ore	2 ore
SIPSE Pay – componenti tecniche	8 ore	2 ore
SMGCGE e SMACG	8 ore	4 ore
Documentazione normativa	24 ore	24 ore

3. I valori costituiscono obiettivi progettuali e non prestazioni già conseguite.
4. Ogni obiettivo deve essere verificato attraverso prove effettive di ripristino.
5. Le funzioni che dipendono da intermediari esterni devono essere valutate anche sulla base degli impegni contrattuali e delle capacità effettive dei rispettivi fornitori.

Articolo 18 – Backup e conservazione

1. Il MSP adotta procedure di backup periodico.
2. Le copie di sicurezza devono essere:
   a. separate dagli ambienti operativi;
   b. protette da accessi non autorizzati;
   c. cifrate ove necessario;
   d. sottoposte a controlli di integrità;
   e. conservate secondo politiche documentate;
   f. periodicamente testate.
3. È raccomandata l'adozione di una strategia 3-2-1:
   - almeno tre copie dei dati;
   - due differenti supporti o ambienti;
   - una copia separata e non direttamente modificabile dall'ambiente operativo.
4. La disponibilità di una copia di backup non equivale alla garanzia di recuperabilità: il ripristino deve essere effettivamente verificato.

Articolo 19 – Infrastrutture alternative

1. Il MSP può predisporre infrastrutture alternative per le funzioni essenziali.
2. Le infrastrutture devono garantire, secondo le risorse effettivamente disponibili:
   a. disponibilità dei dati;
   b. autenticazione;
   c. integrità delle registrazioni;
   d. controllo degli accessi;
   e. tracciabilità;
   f. ripristino delle configurazioni.
3. L'utilizzo di un ambiente alternativo deve essere autorizzato e documentato.
4. Il passaggio all'ambiente alternativo non può generare duplicazioni di registrazioni o attribuzioni.

Articolo 20 – Attivazione della continuità

Il PCO-MSP viene attivato quando un evento:

1. compromette una funzione essenziale;
2. supera le soglie di indisponibilità stabilite;

3. mette a rischio l'integrità dei dati;
4. compromette la sicurezza delle informazioni;
5. impedisce l'esecuzione ordinaria delle procedure;
6. determina un rischio non gestibile attraverso i controlli ordinari.

L'attivazione è registrata mediante verbale con indicazione dell'evento, delle decisioni, dei responsabili e delle misure adottate.

TITOLO VI – SICUREZZA INFORMATICA E PROTEZIONE DEI DATI

Articolo 21 – Sicurezza degli accessi

1. L'accesso ai sistemi è consentito esclusivamente a soggetti autorizzati.
2. Sono previste:
   a. autenticazione individuale;
   b. autenticazione multifattore per gli accessi privilegiati;
   c. gestione delle autorizzazioni secondo il principio del minimo privilegio;
   d. revoca tempestiva degli accessi non più necessari;
   e. registrazione degli accessi;
   f. revisione periodica delle autorizzazioni.
3. È vietato condividere credenziali personali.

Articolo 22 – Protezione delle informazioni

1. Le informazioni sono classificate secondo quattro livelli:

- Pubbliche;
- Interne;
- Riservate;
- Critiche.

2. Ogni livello determina specifiche regole di accesso, conservazione, trasmissione e divulgazione.
3. I dati personali devono essere trattati nel rispetto della normativa applicabile, incluso il Regolamento UE 2016/679 ove applicabile.
4. La protezione dei dati deve comprendere misure tecniche e organizzative adeguate al rischio.

Articolo 23 – Integrità delle registrazioni

1. Le registrazioni del MSP devono consentire la ricostruzione delle operazioni.
2. Ogni registrazione rilevante deve contenere:
   a. identificativo;
   b. data e ora;
   c. soggetto responsabile;
   d. operazione effettuata;

e. stato precedente;
f. stato successivo;
g. evidenze;
h. eventuale autorizzazione.

3. Le modifiche devono lasciare una traccia verificabile.
4. Le registrazioni non possono essere alterate retroattivamente senza evidenza della rettifica.
5. L'utilizzo di registri append-only, firme digitali o strumenti crittografici può essere adottato quale misura aggiuntiva di integrità.

Articolo 24 – Gestione delle vulnerabilità

1. Le infrastrutture devono essere sottoposte a verifiche periodiche.
2. Devono essere previste:
   a. gestione degli aggiornamenti;
   b. individuazione delle vulnerabilità;
   c. valutazione della gravità;
   d. interventi correttivi;
   e. verifiche successive;
   f. documentazione delle eccezioni.
3. Le vulnerabilità critiche devono essere sottoposte a trattamento prioritario.

TITOLO VII – GESTIONE DEGLI INCIDENTI

Articolo 25 – Classificazione degli incidenti

1. Gli incidenti sono classificati in quattro livelli.

Livello 1 – Basso

Evento circoscritto, senza compromissione delle funzioni essenziali.

Livello 2 – Moderato

Evento che determina disservizi limitati o richiede interventi correttivi.

Livello 3 – Elevato

Evento che compromette una funzione rilevante, la sicurezza dei dati o la regolarità di un processo.

Livello 4 – Critico

Evento che compromette la continuità istituzionale, l'integrità delle registrazioni essenziali o la sicurezza complessiva delle infrastrutture.

2. La classificazione deve essere documentata e può essere aggiornata durante la gestione dell'evento.

Articolo 26 – Procedura di gestione

Ogni incidente segue le seguenti fasi:

1. rilevazione;
2. segnalazione;
3. registrazione;
4. classificazione;
5. valutazione dell'impatto;
6. contenimento;
7. eliminazione della causa, ove possibile;
8. ripristino;
9. verifica;
10. chiusura documentale;
11. analisi delle cause;
12. adozione delle misure preventive.

Articolo 27 – Registro degli incidenti

1. È istituito il Registro degli Incidenti del MSP (RIM-MSP).
2. Ogni incidente riceve un identificativo:

MSP-INC-ANNO-NUMERO

3. Il registro comprende:
    - data e ora;
    - struttura interessata;
    - descrizione;
    - classificazione;
    - impatto;
    - misure adottate;
    - tempi di intervento;
    - responsabile;
    - evidenze;
    - causa individuata;
    - azioni correttive;
    - stato di chiusura.
4. Gli incidenti che coinvolgono dati personali, servizi regolamentati o obblighi verso terzi devono essere gestiti anche secondo le disposizioni normative e contrattuali applicabili.

Articolo 28 – Comunicazione degli incidenti

1. Gli incidenti devono essere comunicati ai responsabili competenti.
2. Gli eventi critici devono essere portati tempestivamente all'attenzione del Direttivo SIPSE.
3. La comunicazione verso gli interessati o le autorità competenti avviene quando prevista dalla normativa applicabile.
4. È vietato occultare, alterare o omettere deliberatamente incidenti rilevanti.

TITOLO VIII – RESILIENZA ISTITUZIONALE

Articolo 29 – Principio di resilienza

1. La resilienza istituzionale consiste nella capacità organizzativa del MSP di:
   a. anticipare le criticità;
   b. assorbire gli effetti degli eventi avversi;
   c. mantenere le funzioni essenziali;
   d. adattare le procedure;
   e. ripristinare le attività;
   f. apprendere dagli eventi.
2. La resilienza non è identificata con la sola disponibilità tecnologica, ma comprende anche continuità decisionale, amministrativa, documentale e organizzativa.

Articolo 30 – Continuità degli organi

1. Ogni organo o struttura essenziale deve disporre di una procedura di sostituzione temporanea.
2. La procedura deve identificare:
   a. titolare;
   b. sostituto;
   c. competenze trasferibili;
   d. limiti di delega;
   e. modalità di attivazione;
   f. durata della sostituzione.
3. Le sostituzioni non possono comportare attribuzione automatica di competenze non previste dagli atti istitutivi.

Articolo 31 – Indisponibilità dei responsabili

1. In caso di indisponibilità del responsabile di una funzione essenziale, opera la procedura di sostituzione formalmente approvata.
2. La sostituzione deve essere registrata.
3. Le operazioni straordinarie devono mantenere il principio della doppia verifica ove tecnicamente e organizzativamente possibile.

Articolo 32 – Protezione della documentazione istituzionale

1. Gli atti fondamentali del MSP devono essere conservati in archivi documentali protetti.
2. Devono essere mantenuti:
   a. versione originale;
   b. data di adozione;
   c. identificativo;
   d. eventuali revisioni;
   e. soggetto emanante;

f. stato documentale;
g. evidenza della pubblicazione, ove avvenuta.

3. Nessuna versione successiva può cancellare la tracciabilità di quella precedente.

Articolo 33 – Dipendenze esterne

1. Il MSP individua le dipendenze da fornitori, piattaforme, infrastrutture e servizi esterni.
2. Per ogni dipendenza essenziale devono essere valutati:
   a. livello di criticità;
   b. disponibilità;
   c. condizioni contrattuali;
   d. tempi di ripristino;
   e. rischi di concentrazione;
   f. alternative praticabili;
   g. possibilità di migrazione.
3. Il MSP non può presumere la disponibilità continuativa di servizi forniti da terzi senza un adeguato titolo o impegno documentale.

TITOLO IX – CONTROLLO, MONITORAGGIO E AUDIT

Articolo 34 – Indicatori di rischio

È istituito il sistema degli indicatori di rischio (KRI – Key Risk Indicators).

Gli indicatori comprendono almeno:

1. numero di incidenti;
2. numero di incidenti critici;
3. tempo medio di rilevazione;
4. tempo medio di ripristino;
5. percentuale di backup verificati;
6. percentuale di sistemi sottoposti ad aggiornamento;
7. numero di accessi anomali;
8. numero di vulnerabilità aperte;
9. percentuale di rischi elevati trattati;
10. percentuale di verifiche completate;
11. numero di dipendenze critiche non mitigate;
12. esito delle prove di continuità.

Articolo 35 – Relazione periodica

1. L'UGR-MSP predispone una relazione periodica sullo stato dei rischi.
2. La relazione contiene:
   a. rischi identificati;
   b. rischi critici;
   c. incidenti;

d. misure correttive;
e. stato del PCO-MSP;
f. verifiche effettuate;
g. vulnerabilità;
h. eventuali criticità non risolte;
i. raccomandazioni.

3. La relazione è trasmessa al Direttivo SIPSE.
4. Le criticità urgenti sono comunicate senza attendere la relazione periodica.

Articolo 36 – Audit interno

1. È previsto un programma di audit interno.
2. L'audit verifica:
   a. conformità alle procedure interne;
   b. adeguatezza dei controlli;
   c. correttezza delle registrazioni;
   d. separazione delle funzioni;
   e. gestione delle credenziali;
   f. efficacia dei piani di continuità;
   g. gestione degli incidenti;
   h. attuazione delle raccomandazioni.
3. L'audit deve essere documentato.
4. Le verifiche non possono essere presentate come certificazioni indipendenti se non svolte da organismi competenti e secondo procedure appropriate.

TITOLO X – PROVE, SIMULAZIONI E MIGLIORAMENTO CONTINUO

Articolo 37 – Programma di test

1. Il MSP istituisce un programma di test periodici.
2. Le prove comprendono:
   a. ripristino dei backup;
   b. recupero delle registrazioni;
   c. indisponibilità simulata dei sistemi;
   d. perdita di connettività;
   e. indisponibilità di un responsabile;
   f. compromissione simulata delle credenziali;
   g. ripristino delle infrastrutture;
   h. verifica della catena di comunicazione.
3. Ogni prova produce un rapporto con esito, criticità e interventi necessari.

Articolo 38 – Frequenza delle verifiche

Il programma minimo prevede:

- verifica dei backup: mensile;

- controllo degli accessi: trimestrale;
- revisione del registro rischi: trimestrale;
- simulazione di continuità: semestrale;
- test di ripristino completo: almeno annuale;
- riesame generale del SIGR-MSP: annuale.

Le frequenze possono essere intensificate in funzione del rischio effettivo.

Articolo 39 – Miglioramento continuo

1. Ogni incidente, test o audit deve contribuire al miglioramento del sistema.
2. Le raccomandazioni devono essere:
   a. registrate;
   b. assegnate;
   c. sottoposte a verifica;
   d. chiuse con evidenza documentale.
3. Il Direttivo SIPSE può disporre revisioni straordinarie.

TITOLO XI – REGISTRI E DOCUMENTAZIONE

Articolo 40 – Registri istituiti

Sono istituiti o coordinati nell'ambito del SIGR-MSP:

1. Anagrafe Interna dei Rischi – AIR-MSP;
2. Registro degli Incidenti – RIM-MSP;
3. Registro delle Vulnerabilità – RVM-MSP;
4. Registro delle Prove di Continuità – RPC-MSP;
5. Registro delle Azioni Correttive – RAC-MSP;
6. Registro delle Dipendenze Critiche – RDC-MSP;
7. Registro delle Verifiche e degli Audit – RVA-MSP.

Articolo 41 – Tracciabilità documentale

1. Ogni registro deve avere un responsabile.
2. Ogni documento deve essere identificabile, datato e versionato.
3. Le rettifiche devono mantenere la traccia delle versioni precedenti.
4. La conservazione deve rispettare gli obblighi legali applicabili e le politiche documentali del MSP.

TITOLO XII – LIMITI, SALVAGUARDIE E RESPONSABILITÀ

Articolo 42 – Limiti degli effetti istituzionali

1. Il SIGR-MSP costituisce un sistema interno di organizzazione, prevenzione e controllo.
2. La sua istituzione non determina automaticamente:
   a. riconoscimento internazionale del MSP;
   b. autorizzazione all'esercizio di attività bancarie;
   c. autorizzazione all'esercizio di servizi di pagamento;
   d. riconoscimento di garanzie finanziarie;
   e. certificazione di riserve;
   f. certificazione di fondi o depositi;
   g. riconoscimento di monete aventi corso legale;
   h. attribuzione di poteri pubblicistici verso terzi.
3. Le attività che richiedono autorizzazioni o requisiti specifici possono essere avviate esclusivamente nel rispetto delle disposizioni applicabili.

Articolo 43 – Nessuna presunzione di disponibilità

1. L'inserimento di un bene, di una garanzia o di una disponibilità in un registro interno non ne dimostra automaticamente:
   a. proprietà;
   b. disponibilità effettiva;
   c. libera trasferibilità;
   d. assenza di vincoli;
   e. opponibilità a terzi;
   f. liquidabilità;
   g. escutibilità.
2. Restano applicabili le distinzioni tra dichiarato, documentato, verificato, perfezionato e disponibile.
3. È vietato utilizzare le registrazioni interne per rappresentare come effettivamente disponibili risorse non verificate o non giuridicamente accessibili.

Articolo 44 – Responsabilità

1. Ogni responsabile risponde delle attività svolte nell'ambito delle proprie competenze secondo le disposizioni applicabili.
2. L'omessa segnalazione intenzionale di incidenti, la falsificazione delle evidenze e l'alterazione delle registrazioni costituiscono violazioni delle regole interne e possono determinare sospensione delle funzioni e ulteriori conseguenze previste dalla legge o dagli accordi applicabili.

TITOLO XIII – DISPOSIZIONI FINALI E ATTUATIVE

Articolo 45 – Documenti attuativi

Per l'attuazione del presente Atto sono predisposti:

1. Regolamento operativo SIGR-MSP;
2. Manuale tecnico di gestione dei rischi;

3. Piano di Continuità Operativa PCO-MSP;
4. Piano di Disaster Recovery DRP-MSP;
5. Manuale di gestione degli incidenti;
6. Procedura di classificazione delle informazioni;
7. Procedura di gestione degli accessi;
8. Modelli uniformi di registrazione e reporting;
9. Piano annuale di audit e test.

Articolo 46 – Attuazione progressiva

1. L'attuazione del SIGR-MSP avviene per fasi.
2. Le fasi comprendono:
    - fase I: istituzione organizzativa;
    - fase II: identificazione e registrazione dei rischi;
    - fase III: approvazione delle procedure;
    - fase IV: implementazione dei controlli;
    - fase V: predisposizione delle infrastrutture;
    - fase VI: test e verifiche;
    - fase VII: autorizzazione interna all'operatività delle singole funzioni.
3. Nessuna funzione è considerata pienamente operativa per il solo fatto di essere prevista dal presente Atto.
4. L'attivazione richiede la verifica delle risorse, delle responsabilità, delle procedure, delle infrastrutture e degli eventuali requisiti autorizzativi applicabili.

Articolo 47 – Entrata in vigore

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

La pubblicazione nel repertorio documentale del MSP ne assicura la tracciabilità istituzionale.

Articolo 48 – Clausola di revisione

Il presente Atto è sottoposto a revisione:

- almeno annuale;
- in caso di modifiche organizzative sostanziali;
- in caso di incidenti critici;
- in caso di nuove esigenze tecnologiche;
- in caso di modifiche normative rilevanti.

DISPOSIZIONE CONCLUSIVA

Il Mercato Sovrano dei Popoli riconosce nella prevenzione dei rischi, nella continuità operativa e nella resilienza istituzionale condizioni essenziali per la stabilità e la credibilità del proprio ordinamento economico multilaterale.

La solidità di un sistema non si misura esclusivamente dalla sua capacità di operare in condizioni ordinarie, ma soprattutto dalla sua capacità di individuare le criticità, proteggere le proprie funzioni essenziali, affrontare le interruzioni e ripristinare le attività sulla base di procedure verificabili.

La continuità istituzionale non è assenza di rischio: è capacità organizzata di governarlo.

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

MERCATO SOVRANO DEI POPOLI – MSP

Atto n. 25/MSP

Codice documentale: SIPSE/MSP/ATTO-25

Data di adozione: da determinare con la deliberazione formale.

Sottoscrizione dell'organo competente: _____

Responsabile della conservazione documentale: _____