S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

ATTO N. 26/MSP

REGOLAMENTO OPERATIVO DEL SISTEMA INTEGRATO DI GESTIONE DEI RISCHI E DELLA RESILIENZA DEL MERCATO SOVRANO DEI POPOLI

SIGR-MSP – Regolamento attuativo dell'Atto n. 25/MSP

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

Ambito di applicazione: Mercato Sovrano dei Popoli – MSP.

Codice documentale: SIPSE/MSP/REG-26.

Natura: Regolamento organizzativo, operativo e procedurale.

PREAMBOLO

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

visto l'Atto n. 25/MSP, recante l'istituzione del Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli;

considerata la necessità di rendere effettive e applicabili le disposizioni istitutive del SIGR-MSP;

ritenuto necessario definire procedure uniformi per l'identificazione, la classificazione, la valutazione, il trattamento e il monitoraggio dei rischi;

riconosciuta l'importanza della separazione delle responsabilità, della tracciabilità delle operazioni e dell'indipendenza delle verifiche;

considerata la necessità di integrare i controlli relativi alle garanzie, alle unità monetarie, alle esposizioni, alle registrazioni, ai sistemi informatici e ai servizi operativi;

assumendo quali riferimenti metodologici ISO 31000, ISO 22301, ISO/IEC 27001 e ISO/IEC 27005, nei rispettivi ambiti;

adotta il presente Regolamento.

TITOLO I – ORGANIZZAZIONE OPERATIVA

Articolo 1 – Oggetto

1. Il presente Regolamento disciplina il funzionamento operativo del Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli.
2. Sono disciplinati:
   a. il procedimento di identificazione dei rischi;
   b. la valutazione e la classificazione;
   c. le soglie di attenzione e di intervento;
   d. le procedure di autorizzazione;
   e. la gestione delle anomalie;
   f. le misure preventive e correttive;
   g. il sistema di allerta;
   h. le responsabilità operative;
   i. le verifiche e gli audit;
   j. la rendicontazione istituzionale.
3. Il Regolamento costituisce riferimento obbligatorio per le strutture interne del MSP formalmente assoggettate al sistema.

Articolo 2 – Struttura organizzativa

Il SIGR-MSP si articola nelle seguenti unità:

1. Direttivo SIPSE: supervisione istituzionale e approvazione degli indirizzi;
2. Direzione MSP: coordinamento operativo generale;
3. Unità di Gestione dei Rischi (UGR-MSP): identificazione, valutazione e monitoraggio;
4. Unità di Controllo e Verifica (UCV-MSP): controlli indipendenti e verifiche;
5. Responsabili di Funzione: gestione dei rischi delle rispettive aree;
6. Responsabile della Sicurezza Informatica: protezione delle infrastrutture e delle informazioni;
7. Responsabile della Continuità Operativa: coordinamento del PCO-MSP.

Le funzioni possono essere attribuite a strutture già esistenti, purché siano formalmente individuate e siano rispettati i requisiti di separazione e indipendenza.

Articolo 3 – Responsabilità del Direttivo SIPSE

Il Direttivo SIPSE:

1. approva la politica generale dei rischi;
2. stabilisce i livelli di tolleranza;
3. approva i rischi residui di competenza;
4. riceve le segnalazioni di rischio critico;
5. autorizza le misure straordinarie;
6. esamina le relazioni periodiche;

7. dispone verifiche supplementari;
8. approva le revisioni sostanziali del sistema.

Il Direttivo non sostituisce le verifiche tecniche e non può considerare validata un'operazione per la sola approvazione istituzionale.

Articolo 4 – Unità di Gestione dei Rischi

L'UGR-MSP:

1. mantiene aggiornata l'Anagrafe Interna dei Rischi;
2. assegna gli identificativi;
3. verifica la completezza delle schede;
4. valuta probabilità e impatto;
5. determina il livello di rischio;
6. propone le misure di mitigazione;
7. controlla le scadenze;
8. verifica l'attuazione delle misure;
9. predispone le relazioni;
10. segnala tempestivamente le criticità.

Ogni valutazione deve essere accompagnata da elementi documentali sufficienti.

Articolo 5 – Unità di Controllo e Verifica

L'UCV-MSP:

1. verifica la corretta applicazione del Regolamento;
2. controlla la completezza dei registri;
3. verifica la separazione delle funzioni;
4. esamina le evidenze delle misure correttive;
5. controlla la coerenza tra rischio dichiarato e rischio effettivo;
6. verifica le procedure di autorizzazione;
7. segnala le irregolarità;
8. predispone rapporti di controllo.

L'UCV-MSP non deve dipendere operativamente dai soggetti che sono oggetto delle verifiche.

TITOLO II – PROCEDIMENTO DI GESTIONE DEL RISCHIO

Articolo 6 – Ciclo operativo

Ogni rischio segue un procedimento articolato in dieci fasi:

1. individuazione;
2. registrazione;

3. classificazione;
4. valutazione;
5. determinazione della priorità;
6. predisposizione del piano di trattamento;
7. approvazione;
8. attuazione;
9. verifica;
10. aggiornamento o chiusura.

Nessuna fase può essere considerata completata senza la relativa evidenza documentale.

Articolo 7 – Identificazione dei rischi

I rischi possono essere individuati attraverso:

a. verifiche periodiche;
b. segnalazioni dei responsabili;
c. controlli contabili e amministrativi;
d. verifiche informatiche;
e. audit;
f. incidenti;
g. variazioni organizzative;
h. variazioni normative;
i. nuove attività;
j. introduzione di nuovi strumenti monetari o finanziari;
k. variazioni delle condizioni delle garanzie;
l. dipendenze da soggetti esterni.

Ogni responsabile di funzione è tenuto a segnalare i rischi rilevanti emersi nell'ambito delle proprie attività.

Articolo 8 – Registrazione

1. Ogni rischio è registrato nell'Anagrafe Interna dei Rischi – AIR-MSP.
2. Il codice identificativo segue il formato:

MSP-RISK-2026-0001

3. La registrazione deve contenere almeno:
    - identificativo;
    - data di rilevazione;
    - categoria;
    - descrizione;
    - origine;
    - funzione interessata;
    - responsabile;
    - probabilità;
    - impatto;
    - livello;
    - misure esistenti;

- misure necessarie;
- scadenza;
- stato;
- evidenze.

4. Le registrazioni non possono essere eliminate per occultare eventi o criticità.
5. Le rettifiche devono mantenere la cronologia delle modifiche.

Articolo 9 – Scala di probabilità

La probabilità è valutata utilizzando la seguente scala:

Valore	Classe	Descrizione
1	Rara	Evento eccezionale
2	Improbabile	Evento poco frequente
3	Possibile	Evento plausibile
4	Probabile	Evento atteso in determinate condizioni
5	Molto probabile	Evento ricorrente o imminente

La valutazione deve essere motivata e basata, ove disponibili, su dati storici, indicatori e informazioni verificabili.

Articolo 10 – Scala dell'impatto

L'impatto è determinato considerando conseguenze istituzionali, economiche, operative, tecnologiche, giuridiche e reputazionali.

Valore	Classe	Descrizione
1	Trascurabile	Conseguenze minime
2	Limitato	Disservizio circoscritto
3	Significativo	Compromissione di una funzione
4	Grave	Compromissione di funzioni essenziali
5	Critico	Interruzione sistemica o grave compromissione istituzionale

In presenza di impatti multipli, la valutazione deve considerare la conseguenza più grave ragionevolmente prevedibile.

Articolo 11 – Matrice di classificazione

L'indice è determinato mediante la formula:

R = P × I

Probabilità / Impatto	1	2	3	4	5
5 – Molto probabile	5	10	15	20	25
4 – Probabile	4	8	12	16	20

3 – Possibile	3	6	9	12	15
2 – Improbabile	2	4	6	8	10
1 – Rara	1	2	3	4	5

La classificazione è la seguente:

- 1–4: basso;
- 5–9: moderato;
- 10–15: elevato;
- 16–25: critico.

Articolo 12 – Valutazione del rischio inerente e residuo

1. Il rischio inerente è valutato prima dell'applicazione dei controlli aggiuntivi.
2. Il rischio residuo è valutato dopo aver considerato le misure di mitigazione effettivamente implementate.
3. Non possono essere attribuiti miglioramenti di classificazione a misure soltanto programmate o dichiarate.
4. La valutazione del rischio residuo deve essere supportata da evidenze.
5. I rischi critici residui devono essere sottoposti al Direttivo SIPSE.

TITOLO III – SOGLIE DI ALLERTA E PROCEDURE DI INTERVENTO

Articolo 13 – Livelli di allerta

Sono istituiti quattro livelli di allerta.

LIVELLO VERDE – ORDINARIO

Rischio basso.

- Monitoraggio ordinario.
- Registrazione periodica.
- Controlli programmati.

LIVELLO GIALLO – ATTENZIONE

Rischio moderato.

- Informazione al responsabile di funzione.
- Analisi delle cause.
- Misure preventive.
- Verifica periodica rafforzata.

LIVELLO ARANCIONE – ELEVATO

Rischio elevato.

- Segnalazione all'UGR-MSP.
- Piano di mitigazione obbligatorio.
- Informazione alla Direzione MSP.
- Verifica ravvicinata.
- Possibile sospensione cautelativa della singola attività interessata.

LIVELLO ROSSO – CRITICO

Rischio critico.

- Segnalazione immediata alla Direzione MSP.
- Comunicazione al Direttivo SIPSE.
- Valutazione della sospensione della funzione compromessa.
- Attivazione delle procedure di emergenza, ove necessaria.
- Verifica indipendente.
- Piano di ripristino e contenimento.

Articolo 14 – Tempi interni di segnalazione

I tempi massimi interni di presa in carico sono:

Livello	Prima segnalazione	Presa in carico
Verde	Nel ciclo ordinario	Programmata
Giallo	Entro 5 giorni lavorativi	Entro 5 giorni lavorativi
Arancione	Entro 24 ore	Entro 1 giorno lavorativo
Rosso	Immediata	Senza ritardo

I tempi indicano obiettivi organizzativi interni e non sostituiscono eventuali termini di legge o obblighi di comunicazione più stringenti.

Articolo 15 – Procedura di escalation

1. La struttura che rileva il rischio informa il proprio responsabile.
2. Il responsabile trasmette la segnalazione all'UGR-MSP.
3. L'UGR-MSP procede alla classificazione.
4. Per rischi elevati viene informata la Direzione MSP.
5. Per rischi critici viene informato il Direttivo SIPSE.
6. Ogni passaggio deve essere documentato.
7. In presenza di un pericolo imminente per dati, disponibilità o integrità dei sistemi, il responsabile tecnico può adottare misure temporanee di contenimento, dandone immediata comunicazione ai soggetti competenti.

Articolo 16 – Sospensione cautelativa

1. La sospensione cautelativa può riguardare esclusivamente la funzione, l'operazione o il processo interessato.

2. Deve essere motivata da:
   a. rischio critico;
   b. compromissione dell'integrità;
   c. indisponibilità di garanzie essenziali;
   d. sospetto fondato di frode;
   e. incidente informatico grave;
   f. impossibilità di verificare l'affidabilità dell'operazione.
3. La sospensione è registrata e sottoposta a riesame.
4. La riattivazione richiede la verifica del ripristino delle condizioni di sicurezza.

TITOLO IV – CONTROLLI SULLE ATTIVITÀ DEL MSP

Articolo 17 – Controllo delle unità monetarie

Le unità monetarie registrate nel RMUM sono sottoposte a controlli relativi a:

1. identificazione;
2. denominazione;
3. codice;
4. soggetto emittente o responsabile;
5. metodologia di valorizzazione;
6. documentazione;
7. condizioni di utilizzo;
8. eventuali limiti di conversione;
9. rischi di cambio;
10. stato operativo.

Ogni unità deve essere distinta tra:

- istituita documentalmente;
- registrata;
- tecnicamente implementata;
- disponibile all'utilizzo;
- sottoposta a verifica;
- eventualmente sospesa.

L'iscrizione nel RMUM non costituisce riconoscimento di corso legale, garanzia di convertibilità o autorizzazione finanziaria.

Articolo 18 – Controllo delle garanzie

Le garanzie iscritte nel RMG sono sottoposte a verifica riguardante:

1. identità del soggetto garante;
2. titolarità;
3. esistenza documentale;
4. valore dichiarato;

5. metodologia di valutazione;
6. vincoli;
7. disponibilità;
8. validità temporale;
9. condizioni di escussione;
10. eventuali duplicazioni.

La classificazione documentale deve distinguere:

a. dichiarata;

b. documentata;

c. verificata;

d. giuridicamente perfezionata;

e. disponibile;

f. eventualmente escutibile.

Nessuna garanzia può essere considerata pienamente utilizzabile sulla sola base della sua iscrizione in un registro interno.

Articolo 19 – Controllo delle esposizioni

1. Le esposizioni devono essere registrate e riconciliate.
2. Ogni esposizione deve essere associata alla relativa documentazione.
3. Devono essere verificati:
    - valore;
    - scadenza;
    - controparte;
    - copertura;
    - eventuali concentrazioni;
    - condizioni di regolamento;
    - stato dell'operazione.
4. Le esposizioni prive di documentazione sufficiente devono essere classificate come non verificate.
5. Il sistema non può rappresentare come coperta un'esposizione per la quale la garanzia non risulti effettivamente disponibile e idonea.

Articolo 20 – Controllo SIPSE Pay e dei processi di regolamento

1. I processi tecnici di SIPSE Pay sono sottoposti a controlli di:
   a. autenticazione;
   b. autorizzazione;
   c. integrità delle istruzioni;
   d. tracciabilità;

e. riconciliazione;
f. gestione degli errori;
g. sicurezza;
h. disponibilità.

2. Le operazioni che comportano movimentazione di fondi o prestazione di servizi di pagamento possono essere svolte esclusivamente nel rispetto degli eventuali requisiti autorizzativi applicabili.
3. Il sistema interno di registrazione non sostituisce i sistemi di regolamento e gli intermediari eventualmente necessari.
4. Le operazioni non confermate devono mantenere lo stato di sospese o non regolate.

Articolo 21 – Controllo dei fornitori

1. I fornitori che svolgono funzioni essenziali sono sottoposti a valutazione preventiva.
2. La valutazione considera:
   - affidabilità;
   - sicurezza;
   - continuità;
   - condizioni contrattuali;
   - dipendenze tecnologiche;
   - protezione dei dati;
   - possibilità di sostituzione;
   - modalità di uscita.
3. Per i fornitori critici devono essere previste misure alternative.

TITOLO V – AUTORIZZAZIONI E SEGREGAZIONE

Articolo 22 – Principio delle quattro verifiche

Per le operazioni ad elevata rilevanza organizzativa o economica è adottato un procedimento articolato in quattro passaggi:

1. predisposizione;
2. verifica documentale;
3. autorizzazione;
4. controllo successivo.

Le quattro funzioni devono essere separate ove le dimensioni organizzative lo consentano.

Articolo 23 – Doppia autorizzazione

1. Le operazioni classificate come critiche devono essere sottoposte a doppia autorizzazione.
2. La doppia autorizzazione deve essere effettuata da due soggetti distinti.
3. Le autorizzazioni devono essere individuali, registrate e verificabili.
4. Nessun soggetto può autorizzare un'operazione da lui stesso predisposta senza una verifica indipendente adeguata.

Articolo 24 – Matrice delle competenze

Operazione	Responsabile	Verifica	Approvazione
Registrazione ordinaria	Funzione competente	Controllo interno	Responsabile funzione
Modifica registro critico	Operatore	UCV o verificatore indipendente	Direzione competente
Registrazione garanzia	Responsabile RMG	Verificatore distinto	Organo autorizzato
Variazione unità monetaria	Unità competente	Verifica tecnica e documentale	Organo competente
Sospensione operazione	Responsabile competente	UGR-MSP	Direzione MSP
Gestione incidente critico	Responsabile tecnico	UCV-MSP	Direzione MSP / organo competente
Modifica politica dei rischi	UGR-MSP	UCV-MSP	Direttivo SIPSE

La matrice deve essere completata con i nominativi e gli atti di attribuzione delle competenze.

Articolo 25 – Conflitti di interesse

1. Ogni responsabile deve dichiarare eventuali conflitti di interesse rilevanti.
2. Il soggetto in conflitto non partecipa alla valutazione o autorizzazione dell'operazione interessata, salvo attività strettamente necessarie e formalmente documentate.
3. Le dichiarazioni sono conservate nell'apposito fascicolo.

TITOLO VI – REGISTRI E MODELLI OPERATIVI

Articolo 26 – Anagrafe Interna dei Rischi

L'AIR-MSP costituisce il registro centrale dei rischi.

Ogni scheda deve contenere:

Campo	Contenuto
ID	Codice univoco
Data	Rilevazione
Categoria	Tipologia di rischio
Descrizione	Evento potenziale
Origine	Causa o fonte
P	Probabilità
I	Impatto

R	Indice
Livello	Classe di rischio
Responsabile	Soggetto incaricato
Mitigazione	Misure previste
Scadenza	Termine
Stato	Aperto / trattato / chiuso
Evidenze	Documenti di supporto

Articolo 27 – Registro degli Incidenti

Il RIM-MSP contiene:

1. codice identificativo;
2. data e ora;
3. descrizione;
4. sistemi interessati;
5. classificazione;
6. impatto;
7. responsabile;
8. azioni di contenimento;
9. ripristino;
10. causa;
11. conseguenze;
12. misure correttive;
13. stato di chiusura.

Articolo 28 – Registro delle Vulnerabilità

Il RVM-MSP registra:

1. identificativo;
2. componente interessato;
3. descrizione della vulnerabilità;
4. gravità;
5. data di rilevazione;
6. origine;
7. esposizione;
8. misura correttiva;
9. responsabile;
10. termine;
11. stato;
12. verifica finale.

Articolo 29 – Registro delle Prove di Continuità

Il RPC-MSP documenta:

- tipologia di prova;

- funzione interessata;
- data;
- responsabile;
- scenario;
- risultato atteso;
- risultato ottenuto;
- RTO misurato;
- RPO misurato;
- criticità;
- interventi correttivi;
- approvazione della chiusura.

Articolo 30 – Registro delle Azioni Correttive

Il RAC-MSP contiene:

1. origine della criticità;
2. descrizione;
3. misura correttiva;
4. responsabile;
5. priorità;
6. scadenza;
7. avanzamento;
8. prova di completamento;
9. verifica indipendente;
10. chiusura.

Articolo 31 – Registro delle Dipendenze Critiche

Il RDC-MSP contiene:

1. funzione dipendente;
2. fornitore o infrastruttura;
3. natura della dipendenza;
4. criticità;
5. condizioni contrattuali;
6. tempi di ripristino;
7. alternative;
8. rischi di concentrazione;
9. responsabile;
10. piano di uscita.

Articolo 32 – Registro delle Verifiche e degli Audit

Il RVA-MSP documenta tutte le attività di verifica, le relative evidenze, le anomalie riscontrate e le raccomandazioni formulate.

TITOLO VII – REPORTING E TRASPARENZA

Articolo 33 – Report mensile

L'UGR-MSP predispone un rapporto mensile comprendente:

1. rischi aperti;
2. rischi elevati;
3. rischi critici;
4. incidenti;
5. vulnerabilità;
6. stato delle azioni correttive;
7. indicatori KRI;
8. eventuali sospensioni;
9. misure di mitigazione;
10. criticità da sottoporre al Direttivo.

Articolo 34 – Relazione trimestrale

La relazione trimestrale comprende:

a. andamento generale dei rischi;

b. variazione dei livelli di esposizione;

c. efficacia dei controlli;

d. stato delle infrastrutture;

e. risultati delle verifiche;

f. criticità ricorrenti;

g. dipendenze esterne;

h. raccomandazioni;

i. proposte di miglioramento.

La relazione viene trasmessa al Direttivo SIPSE.

Articolo 35 – Comunicazione istituzionale

1. Le informazioni pubbliche devono essere accurate, verificabili e coerenti con lo stato effettivo delle attività.
2. Le informazioni riservate non possono essere divulgate senza autorizzazione.

3. Il MSP può pubblicare un rapporto sintetico sulla propria gestione dei rischi, purché non siano divulgati dati sensibili o informazioni che compromettano la sicurezza.
4. I dati non ancora verificati devono essere espressamente qualificati come dichiarati, provvisori o in corso di verifica.

TITOLO VIII – VERIFICHE E MIGLIORAMENTO

Articolo 36 – Programma dei controlli

Il programma minimo prevede:

Controllo	Frequenza
Aggiornamento AIR-MSP	Trimestrale
Verifica degli accessi	Trimestrale
Verifica backup	Mensile
Controllo garanzie critiche	Secondo rischio e scadenze
Verifica riconciliazioni	Secondo il ciclo operativo
Controllo vulnerabilità	Continuativo e periodico
Audit interno	Semestrale
Prova continuità	Semestrale
Riesame complessivo	Annuale

Le verifiche possono essere intensificate quando emergono rischi elevati o critici.

Articolo 37 – Non conformità

1. Ogni violazione del Regolamento deve essere registrata.
2. La non conformità viene classificata come:
    - lieve;
    - significativa;
    - grave;
    - critica.
3. Per ciascuna non conformità sono individuate causa, responsabilità, misura correttiva e termine di risoluzione.
4. Le non conformità critiche sono comunicate al Direttivo SIPSE.

Articolo 38 – Riesame

Il SIGR-MSP è sottoposto a riesame annuale e ogniqualvolta si verifichino:

- modifiche sostanziali;
- incidenti critici;
- nuove attività;
- cambiamenti tecnologici;

- variazioni dei rischi;
- modifiche normative rilevanti.

TITOLO IX – DISPOSIZIONI ATTUATIVE

Articolo 39 – Responsabili e nomine

1. La Direzione MSP predispone l'elenco delle funzioni interessate.
2. Il Direttivo SIPSE approva, secondo le proprie competenze, l'attribuzione delle responsabilità.
3. Ogni nomina deve essere documentata mediante atto specifico.
4. Devono essere individuati anche i sostituti dei responsabili delle funzioni essenziali.

Articolo 40 – Avvio operativo

L'attuazione del presente Regolamento avviene attraverso le seguenti fasi:

Fase 1 – Organizzazione

- individuazione delle unità;
- attribuzione delle responsabilità;
- approvazione della matrice delle competenze.

Fase 2 – Censimento

- identificazione dei rischi;
- censimento delle funzioni;
- mappatura delle dipendenze.

Fase 3 – Registrazione

- attivazione AIR-MSP;
- attivazione RIM-MSP;
- attivazione RVM-MSP;
- attivazione degli altri registri.

Fase 4 – Controllo

- introduzione delle soglie;
- attivazione degli indicatori;
- predisposizione dei controlli.

Fase 5 – Verifica

- test;
- audit;
- controllo delle evidenze;
- revisione delle procedure.

Fase 6 – Operatività

- approvazione dei risultati;
- chiusura delle criticità prioritarie;
- autorizzazione interna delle singole funzioni.

Articolo 41 – Formazione

I soggetti incaricati devono ricevere formazione adeguata alle rispettive funzioni.

La formazione riguarda:

1. identificazione dei rischi;
2. gestione degli incidenti;
3. sicurezza informatica;
4. protezione dei dati;
5. continuità operativa;
6. gestione delle garanzie;
7. procedure di autorizzazione;
8. obblighi di segnalazione.

Articolo 42 – Conservazione

Tutti i registri, i verbali, le relazioni e le evidenze devono essere conservati in un sistema documentale controllato, con identificazione della versione, data, responsabile e cronologia delle modifiche.

Articolo 43 – Limiti e conformità normativa

1. Il presente Regolamento disciplina esclusivamente l'organizzazione e i controlli interni del MSP.
2. Non attribuisce autorizzazioni bancarie, finanziarie o di pagamento.
3. Non costituisce attestazione di solvibilità, liquidità, copertura o certificazione di garanzie.
4. Non sostituisce gli obblighi previsti dalla legislazione applicabile.
5. Ogni attività riservata è subordinata al possesso dei requisiti e delle autorizzazioni eventualmente richiesti.

Articolo 44 – Entrata in vigore

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

Articolo 45 – Revisione

Il Regolamento è sottoposto a revisione annuale o straordinaria in caso di modifiche sostanziali dell'organizzazione, dei sistemi, delle attività o del quadro normativo.

DISPOSIZIONE CONCLUSIVA

Con il presente Atto n. 26/MSP il SIPSE disciplina le modalità operative del Sistema Integrato di Gestione dei Rischi e della Resilienza del Mercato Sovrano dei Popoli.

Il Regolamento stabilisce un modello di responsabilità, prevenzione, controllo e verifica fondato sulla documentazione delle attività, sulla separazione delle funzioni e sulla gestione tempestiva delle criticità.

La gestione dei rischi diviene così parte integrante dell'organizzazione del Mercato Sovrano dei Popoli e non una funzione occasionale o meramente amministrativa.

Un sistema affidabile non è quello che dichiara di non avere rischi, ma quello che sa identificarli, misurarli, controllarli e dimostrare le misure adottate.

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

MERCATO SOVRANO DEI POPOLI – MSP

Atto n. 26/MSP

Codice: SIPSE/MSP/REG-26

Data di approvazione: da determinare.

Organo approvante: _____

Responsabile della conservazione documentale: _____