S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

MERCATO SOVRANO DEI POPOLI – MSP

ATTO N. 29/MSP

Istituzione e disciplina del Sistema di Backup e Protezione degli Archivi del Mercato Sovrano dei Popoli (SBPA-MSP)

Codice documentale: SIPSE/MSP/ATTO-29
Sigla del sistema: SBPA-MSP
Classificazione: Atto istituzionale, organizzativo e tecnico
Materia: Protezione dei dati, copie di sicurezza, archiviazione, conservazione e recuperabilità delle informazioni
Ambito: Infrastrutture, registri, applicazioni, archivi e basi dati del MSP
Collegamento normativo: Atti n. 25/MSP, 26/MSP, 27/MSP e 28/MSP

PREAMBOLO

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

nell'ambito dell'organizzazione e dello sviluppo del Mercato Sovrano dei Popoli (MSP);

considerata la necessità di proteggere il patrimonio informativo, documentale, amministrativo e tecnologico del MSP;

riconosciuto che la disponibilità delle informazioni costituisce una condizione essenziale per la continuità delle funzioni istituzionali e per l'affidabilità dei registri;

considerato che la perdita, la corruzione, la modifica non autorizzata o l'indisponibilità dei dati possono compromettere la ricostruzione delle attività e la verificabilità delle registrazioni;

richiamato l'Atto n. 25/MSP, relativo al Sistema di gestione dei rischi, della continuità operativa e della resilienza istituzionale;

richiamato l'Atto n. 26/MSP, relativo al Sistema Integrato di Gestione dei Rischi e della Resilienza del MSP (SIGR-MSP);

richiamato l'Atto n. 27/MSP, relativo al Piano di Continuità Operativa del MSP (PCO-MSP);

richiamato l'Atto n. 28/MSP, relativo al Piano di Disaster Recovery del MSP (DRP-MSP);

ritenuto necessario disciplinare in modo specifico le operazioni di copia, conservazione, protezione, verifica e recupero delle informazioni;

ritenuto altresì necessario assicurare che le copie di sicurezza siano effettivamente disponibili, integre, leggibili e utilizzabili in caso di necessità;

adotta il presente Atto n. 29/MSP.

TITOLO I – ISTITUZIONE E PRINCIPI GENERALI

Articolo 1 – Istituzione dello SBPA-MSP

1. È istituito il **Sistema di Backup e Protezione degli Archivi del Mercato Sovrano dei Popoli**, denominato SBPA-MSP.
2. Lo SBPA-MSP costituisce il sistema organizzativo e tecnico destinato alla protezione, alla duplicazione controllata, alla conservazione e al recupero delle informazioni utilizzate dal MSP.
3. Il sistema si applica alle informazioni:
   a. istituzionali;
   b. amministrative;
   c. organizzative;
   d. economiche;
   e. documentali;
   f. tecnologiche;
   g. informatiche;
   h. relative ai registri;
   i. relative alle attività di controllo e verifica.
4. Lo SBPA-MSP opera in coordinamento con il DRP-MSP e con il SIGR-MSP.
5. La sua attuazione deve essere progressiva, documentata e verificabile.

Articolo 2 – Finalità

Lo SBPA-MSP persegue le seguenti finalità:

1. Prevenire la perdita accidentale o dolosa delle informazioni.
2. Ridurre il rischio di distruzione degli archivi.
3. Garantire la disponibilità di copie di sicurezza aggiornate.
4. Proteggere i dati contro alterazioni e cancellazioni non autorizzate.
5. Assicurare la conservazione di versioni precedenti delle informazioni.
6. Consentire il recupero delle basi dati e dei documenti.
7. Proteggere le informazioni da attacchi informatici e compromissioni tecnologiche.
8. Garantire la tracciabilità delle operazioni di backup.
9. Rendere verificabile la disponibilità delle copie.

10. Supportare il ripristino dei registri istituzionali.
11. Ridurre la dipendenza da un unico fornitore o ambiente tecnologico.
12. Preservare la documentazione necessaria alla ricostruzione delle attività del MSP.

Articolo 3 – Principi fondamentali

Lo SBPA-MSP si fonda sui seguenti principi:

a. Integrità: le copie devono conservare, per quanto verificabile, la corrispondenza con le informazioni di origine.

b. Disponibilità: le copie devono poter essere reperite e utilizzate dai soggetti autorizzati.

c. Riservatezza: l'accesso alle informazioni deve essere limitato alle persone autorizzate.

d. Separazione: le copie devono essere protette rispetto all'ambiente operativo originario.

e. Tracciabilità: ogni operazione significativa deve essere registrata.

f. Recuperabilità: la disponibilità di una copia deve essere verificata mediante prove concrete.

g. Proporzionalità: le misure di protezione devono essere commisurate alla criticità delle informazioni.

h. Responsabilità: ogni operazione deve avere un responsabile individuabile.

i. Verificabilità: le attività devono produrre evidenze documentali e tecniche.

Articolo 4 – Distinzione tra backup, archivio e conservazione

1. Ai fini del presente Atto sono individuate tre categorie distinte.
2. Il **backup** è una copia di sicurezza destinata al recupero di dati e sistemi.
3. L'**archivio** è l'insieme organizzato delle informazioni e dei documenti conservati per esigenze istituzionali, amministrative o operative.
4. La **conservazione documentale** è il processo organizzato destinato a mantenere nel tempo leggibilità, reperibilità, integrità e contesto dei documenti, nel rispetto delle regole applicabili.
5. Una copia di backup non costituisce automaticamente un archivio documentale conforme agli obblighi di conservazione applicabili.
6. La presenza di un documento in un archivio non dimostra automaticamente che ne esista una copia di sicurezza recuperabile.
7. Le tre funzioni devono essere coordinate, ma mantenute concettualmente e operativamente distinte.

Articolo 5 – Ambito di applicazione

1. Lo SBPA-MSP si applica ai sistemi tecnologici e documentali del MSP secondo il loro effettivo stato di implementazione.

2. Sono inclusi, in particolare:
   a. RMUM – Registro Multilaterale delle Unità Monetarie;
   b. RMG – Registro Multilaterale delle Garanzie;
   c. SMRC;
   d. SMGCGE;
   e. SMACG;
   f. SIPSE Pay, limitatamente alle componenti tecniche effettivamente implementate;
   g. archivi degli atti istituzionali;
   h. documentazione amministrativa;
   i. archivi dei contratti e degli accordi;
   j. documentazione relativa ai fornitori;
   k. archivi di sicurezza informatica;
   l. configurazioni e documentazione tecnica;
   m. sistemi di identità e gestione degli accessi.
3. Ogni sistema deve essere inserito nell'inventario dello SBPA-MSP.
4. L'inclusione nell'ambito di applicazione non costituisce attestazione di operatività, certificazione o effettiva disponibilità di copie già predisposte.

TITOLO II – GOVERNANCE E RESPONSABILITÀ

Articolo 6 – Direzione e supervisione

1. La supervisione istituzionale dello SBPA-MSP è attribuita al Direttivo SIPSE nell'ambito delle competenze interne.
2. La Direzione MSP coordina l'attuazione del sistema.
3. La Direzione MSP approva:
   a. le politiche generali di backup;
   b. la classificazione delle informazioni;
   c. le priorità di protezione;
   d. le risorse necessarie;
   e. le eventuali deroghe;
   f. i programmi annuali di verifica.
4. La Direzione riceve periodicamente un rapporto sullo stato di attuazione.

Articolo 7 – Responsabile del Sistema di Backup

1. È istituita la funzione di **Responsabile del Sistema di Backup del MSP (RSB-MSP)**.
2. Il RSB-MSP:
   a. coordina l'applicazione delle politiche di backup;
   b. mantiene aggiornato l'inventario delle copie;
   c. verifica la corretta esecuzione delle procedure;
   d. coordina i responsabili tecnici;
   e. controlla la disponibilità delle copie;
   f. segnala eventuali anomalie;
   g. propone interventi correttivi;

h. predispone il rapporto periodico sullo stato dei backup;
i. coordina le prove di recupero.

3. Il RSB-MSP non può sostituire la verifica indipendente nei casi in cui abbia eseguito direttamente le operazioni oggetto di controllo.

Articolo 8 – Responsabili delle informazioni

1. Per ciascun sistema o archivio deve essere individuato un Responsabile delle Informazioni.
2. Il Responsabile delle Informazioni:
   a. identifica i dati da proteggere;
   b. ne determina la criticità;
   c. propone la frequenza dei backup;
   d. indica i tempi di conservazione;
   e. verifica la completezza delle informazioni;
   f. comunica le modifiche strutturali;
   g. partecipa alle prove di recupero;
   h. verifica i risultati dal punto di vista funzionale e documentale.
3. Il Responsabile deve comunicare tempestivamente ogni modifica che possa incidere sulle procedure di backup.

Articolo 9 – Responsabile della Sicurezza Informatica

1. Il Responsabile della Sicurezza Informatica definisce e verifica le misure di protezione degli ambienti di backup.
2. In particolare, assicura:
   a. controllo degli accessi;
   b. protezione delle credenziali;
   c. cifratura;
   d. separazione degli ambienti;
   e. monitoraggio degli accessi;
   f. gestione delle vulnerabilità;
   g. protezione contro ransomware e cancellazioni malevole;
   h. verifica delle procedure di sicurezza.
3. Le anomalie critiche devono essere comunicate alla Direzione MSP e al RSB-MSP.

Articolo 10 – Unità di Controllo e Verifica

1. L'Unità di Controllo e Verifica del MSP svolge verifiche periodiche sull'attuazione dello SBPA-MSP.
2. Le verifiche riguardano:
   a. esistenza delle copie dichiarate;
   b. coerenza tra inventario e disponibilità effettiva;
   c. esito delle procedure automatiche;
   d. integrità dei campioni;
   e. prove di recupero;
   f. rispetto delle autorizzazioni;
   g. tracciabilità delle operazioni;
   h. gestione delle anomalie.

3. L'Unità di Controllo e Verifica deve poter consultare le evidenze necessarie senza assumere la gestione ordinaria dei backup.

Articolo 11 – Segregazione delle responsabilità

1. Le attività di produzione dei backup, amministrazione degli archivi, gestione delle chiavi e verifica devono essere separate, ove possibile.
2. Per le operazioni critiche è previsto il principio della doppia autorizzazione.
3. Le operazioni di cancellazione definitiva delle copie devono essere sottoposte a controllo rafforzato.
4. Le eventuali deroghe devono essere motivate e registrate.

TITOLO III – CLASSIFICAZIONE DELLE INFORMAZIONI

Articolo 12 – Classi di protezione

1. Le informazioni del MSP sono classificate in quattro livelli.

Livello P1 – Critico

Informazioni la cui perdita o alterazione può compromettere registri essenziali, processi istituzionali prioritari o ricostruzione di operazioni rilevanti.

Livello P2 – Elevato

Informazioni necessarie alla gestione amministrativa, economica, organizzativa e documentale.

Livello P3 – Ordinario

Informazioni di supporto, comunicazioni e documentazione non essenziale nell'immediata fase di emergenza.

Livello P4 – Pubblico

Informazioni destinate alla pubblicazione o alla diffusione pubblica, per le quali resta comunque necessario proteggere integrità, autenticità e disponibilità.

2. La classificazione deve essere attribuita dal Responsabile delle Informazioni e approvata dalla Direzione MSP.

Articolo 13 – Inventario degli archivi

1. È istituito l'Inventario degli Archivi del MSP (IAM-MSP).

2. Per ciascun archivio devono essere indicati:
   a. denominazione;
   b. identificativo;
   c. responsabile;
   d. tipologia;
   e. classificazione;
   f. ubicazione;
   g. formato;
   h. dimensione;
   i. frequenza di aggiornamento;
   j. frequenza del backup;
   k. periodo di conservazione;
   l. modalità di recupero;
   m. eventuali dipendenze;
   n. stato di verifica.
3. L'inventario deve essere aggiornato quando viene creato, modificato, trasferito o dismesso un archivio.

Articolo 14 – Dati essenziali e dati accessori

1. Per ciascun sistema devono essere individuati i dati essenziali necessari al ripristino.
2. Devono essere distinti:
   a. dati primari;
   b. metadati;
   c. log;
   d. configurazioni;
   e. documenti allegati;
   f. dati di controllo;
   g. dati temporanei;
   h. dati di supporto.
3. I dati temporanei possono essere esclusi dalle copie ordinarie soltanto quando la loro ricostruzione sia tecnicamente possibile e documentata.
4. Le configurazioni necessarie al funzionamento di un sistema devono essere incluse nel perimetro di protezione.

TITOLO IV – POLITICA DI BACKUP

Articolo 15 – Adozione della Politica di Backup

1. È istituita la **Politica di Backup del MSP (PB-MSP)**.
2. La PB-MSP definisce:
   a. sistemi da proteggere;
   b. dati da copiare;
   c. frequenza delle copie;
   d. tipologia di backup;
   e. destinazione;
   f. durata della conservazione;

g. protezione crittografica;
h. modalità di verifica;
i. responsabilità;
j. procedure di recupero.

3. La Politica deve essere approvata dalla Direzione MSP e riesaminata almeno annualmente.

Articolo 16 – Modello di protezione 3-2-1-1-0

1. Il MSP assume quale riferimento tecnico il modello 3-2-1-1-0.
2. Il modello prevede:
   a. almeno tre copie complessive dei dati, comprendendo l'originale;
   b. almeno due tipologie di supporto o ambienti distinti;
   c. almeno una copia separata dall'ambiente primario;
   d. almeno una copia offline o protetta da immutabilità;
   e. verifiche periodiche delle copie, con assenza di errori non risolti.
3. Il modello deve essere applicato progressivamente in funzione della criticità e delle risorse disponibili.
4. Per le informazioni P1 è richiesta una particolare attenzione alla separazione degli ambienti e alla protezione contro la cancellazione malevola.
5. La conformità al modello deve essere dimostrata mediante inventario e rapporti di verifica.

Articolo 17 – Tipologie di backup

Il sistema può utilizzare:

1. **Backup completo:** copia integrale dei dati selezionati.
2. **Backup incrementale:** copia delle modifiche intervenute dall'ultima copia utile.
3. **Backup differenziale:** copia delle modifiche intervenute dall'ultimo backup completo.
4. **Backup transazionale:** copia o registrazione dei log necessari a ricostruire lo stato di una base dati.
5. **Backup documentale:** copia degli archivi e dei documenti.
6. **Backup delle configurazioni:** copia dei parametri necessari alla ricostruzione dell'ambiente.
7. **Backup di sistema:** copia di componenti applicative e infrastrutturali.

La scelta deve essere motivata in relazione alla struttura del sistema e ai tempi di recupero richiesti.

Articolo 18 – Frequenza delle copie

1. La frequenza è stabilita in base alla classificazione delle informazioni e agli obiettivi RPO.
2. È adottata la seguente matrice progettuale iniziale:

Classe	Frequenza indicativa	Conservazione operativa indicativa
P1 – Critico	Giornaliera e, ove necessario, più volte al giorno	30 giorni
P2 – Elevato	Giornaliera	30 giorni
P3 – Ordinario	Settimanale	90 giorni

P4 – Pubblico	A ogni pubblicazione o aggiornamento significativo	Versioni storiche secondo politica

3. Le frequenze indicate sono obiettivi organizzativi iniziali e devono essere adeguate alla natura dei sistemi.
4. Per i database con aggiornamenti frequenti possono essere previste copie dei log transazionali con intervalli più brevi.
5. La frequenza effettiva deve essere registrata per ogni sistema.

Articolo 19 – Calendario dei backup

1. Ogni sistema deve disporre di un calendario di backup.
2. Il calendario deve indicare:
   a. data;
   b. ora;
   c. frequenza;
   d. tipologia;
   e. responsabile;
   f. destinazione;
   g. modalità di verifica;
   h. periodo di conservazione.
3. Le operazioni devono essere pianificate evitando, ove possibile, interferenze con i processi ordinari.
4. Gli eventuali backup non eseguiti devono essere segnalati e recuperati secondo una procedura documentata.

Articolo 20 – Backup automatici e manuali

1. Il MSP privilegia, ove tecnicamente possibile, procedure automatiche di backup.
2. Le procedure automatiche devono prevedere:
   a. registrazione dell'esecuzione;
   b. controllo dell'esito;
   c. segnalazione degli errori;
   d. monitoraggio della capacità di archiviazione;
   e. verifica della destinazione.
3. I backup manuali sono ammessi per esigenze specifiche o di emergenza.
4. Ogni backup manuale deve indicare il soggetto che lo ha eseguito e la motivazione.
5. Le copie manuali non possono essere considerate verificate senza un controllo successivo.

TITOLO V – PROTEZIONE DELLE COPIE

Articolo 21 – Separazione delle copie

1. Le copie di sicurezza devono essere separate dall'ambiente di produzione.
2. La separazione può essere:
   a. fisica;

b. logica;
c. amministrativa;
d. geografica;
e. organizzativa.

3. Per i sistemi P1 devono essere previste misure che riducano il rischio di compromissione simultanea dell'ambiente primario e delle copie.
4. La separazione deve essere documentata.

Articolo 22 – Copie immutabili

1. Per gli archivi P1 deve essere valutata l'adozione di copie immutabili.
2. Le copie immutabili devono impedire o rendere controllabile la modifica e la cancellazione durante il periodo di protezione.
3. Devono essere documentati:
   a. tecnologia utilizzata;
   b. durata dell'immutabilità;
   c. modalità di accesso;
   d. soggetti autorizzati;
   e. procedure di recupero;
   f. eventuali eccezioni.
4. L'immutabilità deve essere verificata mediante test e controlli periodici.

Articolo 23 – Copie offline

1. Per le informazioni P1 è prevista la disponibilità di almeno una copia offline, ove tecnicamente ed economicamente sostenibile.
2. La copia offline deve essere mantenuta separata dagli ambienti ordinari.
3. Il collegamento deve avvenire soltanto per operazioni autorizzate.
4. Ogni collegamento deve essere registrato.
5. La copia deve essere verificata prima e dopo le operazioni di aggiornamento o recupero.

Articolo 24 – Cifratura

1. Le copie contenenti informazioni riservate devono essere cifrate secondo standard e modalità tecniche adeguate.
2. La cifratura deve riguardare, ove applicabile:
   a. dati in transito;
   b. dati archiviati;
   c. supporti rimovibili;
   d. archivi esterni;
   e. copie conservate presso fornitori.
3. Le chiavi crittografiche devono essere gestite separatamente dai dati cifrati.
4. La gestione delle chiavi deve prevedere:
   a. autorizzazione;
   b. custodia;
   c. accesso controllato;
   d. rotazione quando necessaria;
   e. revoca;

f. recupero di emergenza;
g. registrazione delle operazioni.

5. La perdita delle chiavi deve essere trattata come un rischio critico per la recuperabilità.

Articolo 25 – Controllo degli accessi

1. L'accesso alle copie è limitato ai soggetti autorizzati.
2. Devono essere applicati:
   a. identificazione individuale;
   b. autenticazione adeguata;
   c. principio del minimo privilegio;
   d. separazione dei ruoli;
   e. revoca degli accessi non più necessari;
   f. registrazione delle operazioni.
3. Le credenziali amministrative devono essere protette e non condivise indiscriminatamente.
4. Gli accessi di emergenza devono essere sottoposti a verifica successiva.

Articolo 26 – Protezione contro ransomware e cancellazioni malevole

1. Lo SBPA-MSP deve prevedere misure specifiche contro attacchi che possano compromettere contemporaneamente dati e copie di sicurezza.
2. Le misure possono comprendere:
   a. separazione delle credenziali;
   b. copie offline;
   c. immutabilità;
   d. monitoraggio delle cancellazioni;
   e. limitazione dei privilegi;
   f. isolamento degli ambienti;
   g. controllo delle modifiche anomale;
   h. procedure di ripristino in ambiente pulito.
3. In presenza di sospetta compromissione, le copie devono essere protette e sottoposte a verifica prima del loro utilizzo.
4. Non è consentito procedere automaticamente al ripristino da una copia potenzialmente compromessa.

TITOLO VI – CONSERVAZIONE E GESTIONE DEGLI ARCHIVI

Articolo 27 – Periodi di conservazione

1. I periodi di conservazione sono definiti in base:
   a. alla finalità;
   b. alla natura dei dati;
   c. alla criticità;

d. agli obblighi applicabili;
e. alle esigenze di ricostruzione;
f. alla disponibilità delle risorse.

2. La durata delle copie di backup non deve essere confusa con la durata di conservazione dei documenti originali.
3. Le copie possono essere eliminate soltanto quando la cancellazione è compatibile con gli obblighi di conservazione e con le esigenze di sicurezza.

Articolo 28 – Versionamento documentale

1. Gli atti e i documenti istituzionali devono essere sottoposti a procedure di versionamento.
2. Il versionamento deve consentire di individuare:
   a. documento originario;
   b. successive revisioni;
   c. data di modifica;
   d. autore o responsabile;
   e. motivazione;
   f. stato del documento;
   g. eventuale sostituzione o annullamento.
3. Le versioni precedenti devono essere conservate secondo la politica documentale applicabile.
4. Le modifiche non devono cancellare la possibilità di ricostruire la storia del documento.

Articolo 29 – Protezione degli atti istituzionali

1. Gli atti del SIPSE e del MSP devono essere inclusi nelle procedure di backup documentale.
2. Per ogni atto devono essere conservati, ove disponibili:
   a. versione approvata;
   b. data;
   c. identificativo;
   d. allegati;
   e. verbale o evidenza di approvazione;
   f. successive modifiche;
   g. versione pubblicata;
   h. eventuali rettifiche.
3. La pubblicazione di un atto non sostituisce la conservazione della versione originale.
4. Devono essere mantenute copie delle versioni approvate e delle relative evidenze documentali.

Articolo 30 – Integrità e autenticità documentale

1. Il MSP può utilizzare impronte crittografiche, firme elettroniche e altri strumenti tecnici per documentare l'integrità dei file.
2. Per ogni documento sottoposto a controllo di integrità possono essere registrati:
   a. identificativo;
   b. nome del file;
   c. formato;
   d. dimensione;
   e. impronta crittografica;

f. data di acquisizione;
g. versione;
h. ubicazione.

3. L'impronta crittografica consente di rilevare modifiche rispetto al contenuto verificato, ma non dimostra da sola l'autenticità dell'autore o la validità giuridica del documento.
4. La validità delle firme e delle attestazioni deve essere verificata secondo le regole applicabili.

Articolo 31 – Migrazione dei formati

1. Per i documenti destinati alla conservazione nel lungo periodo deve essere valutato il rischio di obsolescenza dei formati.
2. Il MSP può predisporre procedure di migrazione verso formati maggiormente leggibili o supportati.
3. Ogni migrazione deve:
   a. conservare l'originale;
   b. produrre una copia derivata;
   c. documentare il formato di partenza;
   d. documentare il formato di destinazione;
   e. registrare la data;
   f. verificare la leggibilità;
   g. conservare le evidenze.
4. La migrazione non deve comportare la perdita ingiustificata di contenuti, metadati o informazioni contestuali.

Articolo 32 – Cancellazione e dismissione

1. La cancellazione delle copie deve essere effettuata secondo una procedura autorizzata.
2. La procedura deve verificare:
   a. scadenza del periodo di conservazione;
   b. assenza di obblighi contrari;
   c. assenza di blocchi o contestazioni;
   d. disponibilità delle copie sostitutive;
   e. autorizzazione del responsabile.
3. La cancellazione deve essere registrata.
4. I supporti dismessi devono essere sottoposti a procedure adeguate di cancellazione sicura o distruzione.
5. La dismissione deve produrre un'evidenza documentale.

TITOLO VII – REGISTRI E SISTEMI PRIORITARI

Articolo 33 – Protezione del RMUM

1. Il RMUM è classificato, in via progettuale, tra gli archivi P1.

2. Devono essere protetti:
   a. schede delle unità monetarie;
   b. codici;
   c. denominazioni;
   d. identificativi;
   e. versioni;
   f. documenti associati;
   g. cronologia delle modifiche;
   h. stati di registrazione;
   i. evidenze di verifica.
3. Le copie devono consentire la ricostruzione della cronologia delle registrazioni.
4. Ogni recupero deve essere sottoposto a riconciliazione.
5. La presenza di una registrazione nel backup non costituisce prova autonoma della validità dell'unità monetaria, della sua accettazione o del suo valore.

Articolo 34 – Protezione del RMG

1. Il RMG è classificato, in via progettuale, tra gli archivi P1.
2. Devono essere protetti:
   a. schede delle garanzie dichiarate;
   b. identificativi;
   c. documenti allegati;
   d. soggetti dichiaranti;
   e. stati di verifica;
   f. cronologia;
   g. eventuali contestazioni;
   h. aggiornamenti;
   i. evidenze di controllo.
3. Il backup deve preservare la distinzione tra garanzie dichiarate, documentate, verificate e contestate.
4. Il recupero dei dati non determina automaticamente validità, disponibilità, opponibilità o escutibilità delle garanzie.

Articolo 35 – Protezione dello SMRC

1. Le componenti dello SMRC devono essere incluse nel sistema di backup in relazione alle funzioni effettivamente implementate.
2. Devono essere protetti dati, configurazioni, documentazione, log e interfacce.
3. Il responsabile deve predisporre una procedura di recupero specifica.

Articolo 36 – Protezione dello SMGCGE e dello SMACG

1. Le componenti effettivamente implementate dello SMGCGE e dello SMACG sono incluse nel perimetro dello SBPA-MSP.
2. Per ciascun sistema devono essere individuati:
   a. dati essenziali;
   b. configurazioni;
   c. archivi;
   d. log;

e. dipendenze;
f. procedure di recupero;
g. responsabili.

3. Le elaborazioni e le registrazioni devono poter essere ricostruite senza duplicazioni non controllate.

Articolo 37 – Protezione delle componenti tecniche SIPSE Pay

1. Le componenti tecniche di SIPSE Pay sono incluse nel sistema di backup secondo il loro effettivo stato di implementazione.
2. Devono essere protetti, ove presenti:
   a. database;
   b. configurazioni;
   c. log;
   d. identificativi delle operazioni;
   e. registrazioni di stato;
   f. interfacce;
   g. moduli di riconciliazione;
   h. documentazione tecnica.
3. Le operazioni rimaste in stato incerto devono essere identificate e riconciliate prima della riattivazione.
4. Le copie non devono essere utilizzate per generare automaticamente nuove disposizioni o ripetere operazioni già eseguite.
5. Il presente articolo disciplina esclusivamente la protezione tecnica delle informazioni e non attribuisce autorizzazioni all'esercizio di servizi bancari, finanziari o di pagamento.

TITOLO VIII – VERIFICA E RECUPERABILITÀ

Articolo 38 – Distinzione degli stati del backup

Ogni copia deve essere classificata secondo uno dei seguenti stati:

Stato 1 – Pianificato: copia prevista ma non ancora eseguita.

Stato 2 – Eseguito: copia prodotta dal sistema.

Stato 3 – Verificato: copia sottoposta a controllo tecnico di integrità o completezza.

Stato 4 – Recuperato in prova: copia utilizzata con successo in una procedura di ripristino controllata.

Stato 5 – Recuperabilità dimostrata: copia recuperata e sottoposta a validazione tecnica e funzionale documentata.

Una copia non può essere classificata come recuperabile esclusivamente perché il processo di backup ha restituito un esito positivo.

Articolo 39 – Verifica automatica

1. Le procedure di backup devono produrre un rapporto di esecuzione.
2. Il rapporto deve indicare:
   a. data e ora;
   b. sistema;
   c. quantità di dati;
   d. destinazione;
   e. durata;
   f. esito;
   g. eventuali errori;
   h. identificativo della copia.
3. Gli errori devono essere segnalati ai responsabili.
4. Il mancato completamento di un backup P1 deve essere trattato come anomalia prioritaria.

Articolo 40 – Verifica dell'integrità

1. Le copie devono essere sottoposte a controlli periodici.
2. I controlli possono comprendere:
   a. checksum;
   b. hash crittografici;
   c. verifica dei metadati;
   d. confronto delle dimensioni;
   e. test di lettura;
   f. controlli di coerenza;
   g. verifica della struttura degli archivi.
3. Gli esiti devono essere registrati.
4. In caso di differenze non spiegate, la copia deve essere posta in stato di verifica e non utilizzata per il ripristino ordinario.

Articolo 41 – Prove di recupero

1. Il MSP deve effettuare prove periodiche di recupero.
2. Le prove devono comprendere:
   a. recupero di singoli documenti;
   b. recupero di archivi;
   c. ripristino di database;
   d. recupero di configurazioni;
   e. ripristino di sistemi selezionati;
   f. verifica delle copie offline;
   g. verifica delle copie immutabili.
3. Le prove devono essere svolte in ambiente controllato.
4. I risultati devono essere documentati.

Articolo 42 – Frequenza minima delle verifiche

È adottato il seguente calendario iniziale:

Attività	Frequenza progettuale
Controllo degli esiti automatici	Continuativo o a ogni esecuzione
Revisione dei log di backup	Almeno mensile
Verifica campione di copie P1	Almeno mensile
Prova di recupero di documenti P1	Almeno trimestrale
Prova di recupero di database P1	Almeno semestrale
Verifica delle copie offline	Almeno semestrale
Verifica delle copie immutabili	Almeno semestrale
Revisione della Politica di Backup	Almeno annuale

2. Le frequenze possono essere aumentate in base ai rischi.
3. Ogni prova deve essere registrata nel Registro delle Prove di Backup e Recupero.

Articolo 43 – Esiti negativi

1. Una prova con esito negativo deve generare una segnalazione.
2. La segnalazione deve contenere:
   a. copia interessata;
   b. sistema di origine;
   c. problema rilevato;
   d. possibile causa;
   e. impatto;
   f. responsabile;
   g. azione correttiva;
   h. termine di risoluzione.
3. Le copie non recuperabili devono essere chiaramente identificate.
4. La Direzione MSP deve ricevere comunicazione delle anomalie critiche.
5. La chiusura dell'anomalia richiede una nuova verifica positiva.

TITOLO IX – REGISTRI E DOCUMENTAZIONE DEL SISTEMA

Articolo 44 – Registro dei Backup

1. È istituito il **Registro dei Backup del MSP (RB-MSP)**.
2. Il Registro contiene almeno:
   a. identificativo della copia;
   b. sistema di origine;
   c. archivio interessato;
   d. data e ora;
   e. tipologia;
   f. dimensione;

g. destinazione;
h. responsabile;
i. esito;
j. verifica effettuata;
k. stato di recuperabilità;
l. periodo di conservazione.

3. Il Registro deve consentire di individuare rapidamente le copie disponibili per ogni sistema.

Articolo 45 – Registro delle Verifiche

1. È istituito il **Registro delle Verifiche di Backup (RVB-MSP)**.
2. Il Registro contiene:
   a. identificativo della copia;
   b. data della verifica;
   c. metodo utilizzato;
   d. responsabile;
   e. esito;
   f. anomalie;
   g. misure correttive;
   h. eventuale nuova verifica.

Articolo 46 – Registro delle Prove di Recupero

1. È istituito il **Registro delle Prove di Backup e Recupero (RPBR-MSP)**.
2. Il Registro contiene:
   a. programma delle prove;
   b. sistema interessato;
   c. copia utilizzata;
   d. data;
   e. procedura;
   f. tempi effettivi;
   g. risultato;
   h. anomalie;
   i. responsabili;
   j. approvazione dell'esito.
3. Il Registro deve essere coordinato con il Registro delle Prove di Disaster Recovery previsto dall'Atto n. 28/MSP.

Articolo 47 – Registro delle Cancellazioni

1. È istituito il **Registro delle Cancellazioni delle Copie (RCC-MSP)**.
2. Il Registro documenta:
   a. copia eliminata;
   b. motivazione;
   c. periodo di conservazione;
   d. autorizzazione;
   e. responsabile;
   f. modalità di cancellazione;

g. data;
h. esito.

3. Le cancellazioni delle copie P1 sono sottoposte a doppia autorizzazione.

Articolo 48 – Fascicolo dello SBPA-MSP

1. È istituito il Fascicolo Tecnico dello SBPA-MSP.
2. Il Fascicolo comprende:
   a. Politica di Backup;
   b. inventario degli archivi;
   c. inventario delle copie;
   d. calendario;
   e. procedure tecniche;
   f. rapporti automatici;
   g. rapporti di verifica;
   h. test di recupero;
   i. autorizzazioni;
   j. anomalie;
   k. misure correttive;
   l. revisioni.
3. Il Fascicolo deve essere aggiornato e conservato in ambiente protetto.

TITOLO X – GESTIONE DEGLI INCIDENTI E DELLE EMERGENZE

Articolo 49 – Segnalazione di anomalie

1. Ogni anomalia relativa alle copie deve essere segnalata al RSB-MSP.
2. Sono considerate anomalie rilevanti:
   a. backup non eseguito;
   b. copia incompleta;
   c. errore di lettura;
   d. perdita di una copia;
   e. accesso non autorizzato;
   f. cancellazione anomala;
   g. alterazione;
   h. perdita di una chiave;
   i. indisponibilità dell'archivio;
   j. sospetta compromissione informatica.
3. Le anomalie critiche devono essere comunicate immediatamente alla Direzione MSP e al Responsabile della Sicurezza Informatica.

Articolo 50 – Protezione delle copie durante un incidente

1. In caso di incidente informatico, le copie devono essere protette da ulteriori modifiche o cancellazioni.
2. Il Responsabile della Sicurezza Informatica può disporre l'isolamento degli ambienti interessati.
3. Le copie sospette devono essere poste in quarantena.
4. Prima del recupero deve essere verificata l'assenza di compromissioni note.
5. Il ripristino deve avvenire secondo le procedure del DRP-MSP.

Articolo 51 – Perdita o compromissione delle copie

1. La perdita di una copia P1 costituisce anomalia critica.
2. Il responsabile deve:
   a. segnalare l'evento;
   b. identificare le copie alternative;
   c. verificare l'eventuale impatto sui dati;
   d. valutare la necessità di nuove copie;
   e. proporre misure compensative;
   f. documentare l'evento.
3. Qualora non esista una copia recuperabile, la Direzione MSP deve valutare le conseguenze e disporre le misure necessarie.
4. La situazione deve essere riportata nel registro dei rischi del MSP.

TITOLO XI – FORNITORI E SERVIZI ESTERNI

Articolo 52 – Gestione dei fornitori

1. I fornitori che ospitano o gestiscono copie e archivi devono essere individuati nell'inventario delle dipendenze tecnologiche.
2. Devono essere valutati:
   a. affidabilità del servizio;
   b. modalità di backup;
   c. ubicazione dei dati;
   d. misure di sicurezza;
   e. possibilità di esportazione;
   f. tempi di recupero dichiarati;
   g. modalità di cessazione del rapporto;
   h. procedure di restituzione dei dati.
3. Le informazioni fornite dai fornitori devono essere distinte dalle verifiche eseguite direttamente dal MSP.

Articolo 53 – Accordi e responsabilità

1. I rapporti con i fornitori devono essere disciplinati da accordi coerenti con la natura del servizio.

2. Gli accordi devono prevedere, ove applicabile:
   a. obblighi di riservatezza;
   b. misure di sicurezza;
   c. gestione degli incidenti;
   d. disponibilità delle copie;
   e. modalità di recupero;
   f. esportazione dei dati;
   g. restituzione o cancellazione;
   h. collaborazione nelle verifiche.
3. La responsabilità del fornitore non elimina la necessità di controlli da parte del MSP.

Articolo 54 – Portabilità e indipendenza

1. Il MSP deve evitare, per quanto possibile, dipendenze tecnologiche che impediscano il recupero o l'esportazione dei dati.
2. I sistemi devono essere progettati per consentire, ove tecnicamente praticabile:
   a. esportazione dei dati;
   b. accesso alle copie;
   c. recupero in ambiente alternativo;
   d. trasferimento a un diverso fornitore;
   e. ricostruzione delle configurazioni essenziali.
3. Le modalità di portabilità devono essere testate periodicamente.

TITOLO XII – CONTROLLO, AUDIT E MIGLIORAMENTO

Articolo 55 – Controllo periodico

1. L'Unità di Controllo e Verifica svolge controlli periodici sullo SBPA-MSP.
2. Le verifiche devono considerare:
   a. copertura dei sistemi;
   b. esecuzione dei backup;
   c. disponibilità delle copie;
   d. integrità;
   e. recuperabilità;
   f. protezione degli accessi;
   g. aggiornamento dei registri;
   h. gestione delle anomalie.
3. I controlli devono essere documentati.

Articolo 56 – Indicatori di efficacia

Sono istituiti i seguenti indicatori:

1. percentuale di sistemi censiti;

2. percentuale di sistemi P1 coperti da backup;
3. percentuale di backup completati;
4. percentuale di copie verificate;
5. percentuale di copie recuperabili;
6. numero di prove eseguite;
7. percentuale di prove con esito positivo;
8. numero di anomalie critiche;
9. tempo medio di risoluzione delle anomalie;
10. percentuale di archivi con responsabile assegnato;
11. percentuale di copie separate dall'ambiente primario;
12. percentuale di copie protette da immutabilità o offline.

Gli indicatori devono essere valorizzati sulla base di dati effettivi, senza attribuire risultati non dimostrati.

Articolo 57 – Rapporto periodico

1. Il RSB-MSP predispone un rapporto periodico sullo stato del sistema.
2. Il rapporto deve contenere:
   a. sistemi protetti;
   b. sistemi non ancora protetti;
   c. copie eseguite;
   d. copie verificate;
   e. prove di recupero;
   f. anomalie;
   g. interventi correttivi;
   h. risorse necessarie;
   i. stato di attuazione.
3. Il rapporto è trasmesso alla Direzione MSP.

Articolo 58 – Revisione annuale

1. La Politica di Backup è sottoposta a revisione almeno annuale.
2. La revisione è anticipata in caso di:
   a. nuovi sistemi;
   b. incidenti;
   c. cambiamento dei fornitori;
   d. modifiche infrastrutturali;
   e. nuove esigenze di conservazione;
   f. esito negativo dei test;
   g. modifiche normative.
3. Le revisioni devono essere versionate.

TITOLO XIII – ATTUAZIONE PROGRESSIVA

Articolo 59 – Fasi di attuazione

L'attuazione dello SBPA-MSP è articolata in cinque fasi.

FASE 1 – Censimento

- identificazione degli archivi;
- individuazione dei responsabili;
- classificazione delle informazioni;
- inventario dei sistemi.

FASE 2 – Protezione

- definizione della Politica di Backup;
- predisposizione delle copie;
- separazione degli ambienti;
- gestione delle credenziali;
- protezione delle chiavi.

FASE 3 – Verifica

- controllo automatico;
- verifica dell'integrità;
- verifica della leggibilità;
- controllo delle copie offline;
- controllo delle copie immutabili.

FASE 4 – Recupero

- prove di ripristino;
- recupero di database;
- recupero degli archivi;
- validazione delle informazioni;
- registrazione dei risultati.

FASE 5 – Consolidamento

- audit;
- risoluzione delle anomalie;
- aggiornamento degli inventari;
- revisione degli obiettivi;
- rapporto annuale.

Articolo 60 – Priorità di attuazione

1. La prima priorità è assegnata alle informazioni classificate P1.
2. L'ordine iniziale di attuazione è il seguente:
   a. atti istituzionali e documentazione fondamentale;
   b. RMUM;
   c. RMG;

d. sistemi di identità e accesso;
e. SMRC;
f. SMGCGE;
g. SMACG;
h. componenti tecniche SIPSE Pay;
i. archivi amministrativi;
j. documentazione ordinaria.

3. La Direzione MSP può modificare l'ordine sulla base della valutazione dei rischi.
4. Ogni priorità deve essere motivata e registrata.

Articolo 61 – Piano annuale delle attività

1. Il RSB-MSP predispone il Piano annuale delle attività.
2. Il documento deve indicare:
   a. sistemi interessati;
   b. interventi;
   c. responsabili;
   d. risorse;
   e. scadenze;
   f. prove;
   g. indicatori;
   h. risultati attesi.
3. Le attività non completate devono essere indicate come tali.
4. Il completamento di un'attività deve essere accompagnato da un'evidenza verificabile.

TITOLO XIV – RIFERIMENTI METODOLOGICI E LIMITI

Articolo 62 – Riferimenti tecnici

1. Lo SBPA-MSP può utilizzare come riferimenti metodologici:
   a. ISO/IEC 27001, per la gestione della sicurezza delle informazioni;
   b. ISO/IEC 27002, per i controlli di sicurezza;
   c. ISO/IEC 27031, per la preparazione delle tecnologie alla continuità;
   d. ISO 22301, per la continuità operativa;
   e. NIST Cybersecurity Framework;
   f. NIST SP 800-34, per la pianificazione della contingenza;
   g. NIST SP 800-88, per la sanitizzazione dei supporti;
   h. NIST SP 800-209, per la sicurezza dello storage.
2. I riferimenti sono utilizzati come strumenti di progettazione e miglioramento.
3. Il loro richiamo non equivale a certificazione o attestazione di conformità.

Articolo 63 – Limiti di efficacia

1. Il presente Atto istituisce il quadro organizzativo e tecnico interno dello SBPA-MSP.

2. L'adozione formale non dimostra automaticamente:
   a. l'esistenza di copie effettivamente eseguite;
   b. la disponibilità di infrastrutture alternative;
   c. l'esistenza di archivi immutabili;
   d. la disponibilità di copie offline;
   e. la riuscita delle procedure di recupero;
   f. la conformità certificata a standard internazionali.
3. L'effettiva attuazione deve essere dimostrata mediante inventari, rapporti, registri, prove e verifiche.
4. Ogni dichiarazione pubblica sul livello di protezione raggiunto deve essere coerente con le evidenze disponibili.

Articolo 64 – Entrata in vigore

1. Il presente Atto entra in vigore dalla data della sua approvazione secondo le procedure interne del SIPSE.
2. La Direzione MSP è incaricata del coordinamento generale.
3. Il RSB-MSP è incaricato della predisposizione della Politica di Backup e dei registri previsti.
4. I responsabili dei sistemi devono collaborare alla ricognizione e alla protezione delle informazioni.
5. Le strutture interessate devono documentare lo stato effettivo di attuazione.

ALLEGATO A – DOCUMENTI OPERATIVI DELLO SBPA-MSP

Codice	Documento	Finalità
SBPA-01	Politica di Backup del MSP	Regole generali
SBPA-02	Inventario degli Archivi	Censimento
SBPA-03	Inventario delle Copie	Identificazione dei backup
SBPA-04	Calendario dei Backup	Programmazione
SBPA-05	Registro dei Backup (RB-MSP)	Tracciabilità
SBPA-06	Registro delle Verifiche (RVB-MSP)	Controllo integrità
SBPA-07	Registro delle Prove di Recupero (RPBR-MSP)	Recuperabilità
SBPA-08	Registro delle Cancellazioni (RCC-MSP)	Controllo eliminazioni
SBPA-09	Procedura di Protezione delle Chiavi	Sicurezza crittografica
SBPA-10	Procedura di Recupero Archivi	Ripristino documentale
SBPA-11	Procedura di Verifica Integrità	Controlli tecnici
SBPA-12	Rapporto Periodico SBPA	Rendicontazione

ALLEGATO B – MODELLO DI REGISTRAZIONE DI UN BACKUP

Identificativo backup: _____

Sistema di origine: _____

Archivio: _____

Classificazione: P1 / P2 / P3 / P4

Data e ora: _____

Tipologia: Completo / Incrementale / Differenziale / Transazionale / Documentale

Responsabile: _____

Destinazione: _____

Dimensione: _____

Esito dell'esecuzione: Positivo / Negativo / Parziale

Verifica di integrità: Positiva / Negativa / Non eseguita

Copia immutabile: Sì / No

Copia offline: Sì / No

Cifratura: Sì / No

Periodo di conservazione: _____

Stato della copia: Pianificato / Eseguito / Verificato / Recuperato in prova / Recuperabilità dimostrata

Anomalie: _____

Firma del responsabile: _____

ALLEGATO C – MODELLO DI VERIFICA DELLA RECUPERABILITÀ

Identificativo della prova: _____

Sistema: _____

Copia selezionata: _____

Data della prova: _____

Ambiente utilizzato: _____

Responsabile tecnico: _____

Verificatore: _____

Controlli eseguiti

- Lettura della copia.
- Verifica dell'integrità.
- Verifica dei metadati.
- Recupero dei dati.
- Verifica della struttura.
- Verifica funzionale.
- Confronto con le informazioni originarie.
- Verifica delle autorizzazioni.

Tempo effettivo di recupero: _____

Risultato: Positivo / Negativo / Parziale

Anomalie: _____

Azioni correttive: _____

Conclusione: Recuperabilità dimostrata / Recuperabilità non dimostrata

Firma del responsabile: _____

Firma del verificatore: _____

ALLEGATO D – MATRICE DI STATO DELLA PROTEZIONE

Stato	Descrizione	Evidenza richiesta
0	Nessun backup documentato	Nessuna
1	Backup pianificato	Politica e calendario
2	Backup eseguito	Rapporto di esecuzione
3	Backup verificato	Rapporto di integrità

4	Recupero testato	Verbale di prova
5	Recuperabilità dimostrata	Rapporto tecnico e validazione

Principio generale: nessun sistema può essere dichiarato pienamente protetto sulla sola base della pianificazione di un backup o dell'esito positivo della sua esecuzione.

DISPOSIZIONE CONCLUSIVA

Con il presente Atto n. 29/MSP, il SIPSE istituisce il Sistema di Backup e Protezione degli Archivi del Mercato Sovrano dei Popoli.

Lo SBPA-MSP costituisce lo strumento destinato a proteggere il patrimonio informativo del MSP, assicurando una disciplina comune per la produzione delle copie, la loro conservazione, la protezione contro alterazioni e cancellazioni, la verifica dell'integrità e la dimostrazione della recuperabilità.

La protezione delle informazioni viene così inserita in un sistema organizzato di responsabilità, registrazioni, controlli e verifiche.

S.I.P.S.E. – MERCATO SOVRANO DEI POPOLI

Ogni informazione deve essere protetta. Ogni copia deve essere verificata. Ogni recupero deve essere dimostrabile.