SIPSE

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

ATTO N. 37/MSP

REGOLAMENTO DI CONSERVAZIONE, ARCHIVIAZIONE E PROTEZIONE DEL PATRIMONIO DOCUMENTALE SIPSE–MSP

Codice documentale: SIPSE-MSP-ATTO-037-V1.0
Data di emissione: 18 novembre 2026
Versione: 1.0
Stato: Testo predisposto per approvazione
Ambito: SIPSE – Mercato Sovrano dei Popoli
Classificazione: Regolamentare – Organizzativa – Tecnica

PREAMBOLO

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

considerata la necessità di assicurare la conservazione permanente e organizzata della memoria documentale istituzionale;

considerata la rilevanza degli atti, dei regolamenti, delle deliberazioni, dei registri e delle evidenze prodotte nell'ambito del Mercato Sovrano dei Popoli;

richiamato l'Atto n. 35/MSP, recante il Regolamento generale di gestione, aggiornamento e controllo della documentazione;

richiamato l'Atto n. 36/MSP, recante il Sistema di Codificazione, Identificazione e Classificazione degli Atti e dei Documenti;

riconosciuta la necessità di proteggere la documentazione contro perdita, deterioramento, alterazione, distruzione e accesso non autorizzato;

considerata l'esigenza di assicurare la disponibilità e la recuperabilità dei documenti anche in situazioni di emergenza o interruzione dei sistemi informatici;

ritenuto necessario istituire un sistema coordinato di archiviazione, conservazione, protezione, backup e verifica dell'integrità;

ADOTTA IL PRESENTE REGOLAMENTO.

TITOLO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto

1. Il presente Regolamento disciplina il sistema di conservazione, archiviazione e protezione del patrimonio documentale SIPSE e MSP.
2. Sono disciplinate:
   a. l'organizzazione degli archivi;
   b. la classificazione documentale;
   c. la conservazione dei documenti;
   d. la protezione degli originali;
   e. la gestione delle copie;
   f. la conservazione digitale;
   g. il backup e il ripristino;
   h. il controllo dell'integrità;
   i. la gestione degli accessi;
   j. la continuità della memoria documentale;
   k. la dismissione e lo scarto autorizzato;
   l. la verifica delle attività archivistiche.
3. Il sistema si applica alla documentazione istituzionale, normativa, amministrativa, economica, finanziaria, tecnica e operativa.

Art. 2 – Finalità

1. Il presente Regolamento persegue le seguenti finalità:

   a. preservare il patrimonio documentale SIPSE;

   b. garantire la reperibilità degli atti;

   c. impedire la perdita incontrollata di documentazione;

   d. assicurare la conservazione delle versioni originali;

   e. garantire la ricostruzione della storia documentale;

   f. proteggere le informazioni riservate;

   g. assicurare la continuità di accesso ai documenti;

   h. predisporre sistemi di recupero in caso di incidente;

   i. garantire l'integrità dei documenti digitali;

   j. mantenere una memoria istituzionale organizzata e verificabile.

Art. 3 – Ambito di applicazione

1. Il Regolamento si applica a tutte le strutture e funzioni SIPSE e MSP che producono, ricevono, utilizzano o conservano documentazione nell'ambito delle rispettive competenze.
2. Sono compresi:
   a. atti istitutivi;
   b. regolamenti;
   c. deliberazioni;
   d. decreti;
   e. determinazioni;
   f. procedure;
   g. manuali;
   h. protocolli;
   i. registri;
   j. modelli operativi;
   k. rapporti di monitoraggio;
   l. relazioni tecniche;
   m. dossier;
   n. documentazione economica e finanziaria;
   o. documentazione informatica;
   p. corrispondenza istituzionale;
   q. evidenze delle attività svolte.
3. Il presente Regolamento si applica indipendentemente dal supporto utilizzato.

Art. 4 – Principi di conservazione

1. La conservazione documentale si fonda sui seguenti principi:
   a. autenticità;
   b. integrità;
   c. affidabilità;
   d. leggibilità;
   e. reperibilità;
   f. disponibilità;
   g. riservatezza;
   h. tracciabilità;
   i. continuità;
   j. protezione nel tempo.
2. La conservazione deve consentire di ricostruire l'origine, la versione, la provenienza e la storia di ciascun documento.
3. La semplice memorizzazione di un file non equivale automaticamente a un processo di conservazione digitale a norma.

TITOLO II – ORGANIZZAZIONE DEL SISTEMA ARCHIVISTICO

Art. 5 – Istituzione dell'Archivio Documentale SIPSE

1. È istituito l'Archivio Documentale SIPSE (ADS-SIPSE).
2. L'Archivio costituisce il sistema organizzato di raccolta, classificazione, conservazione e consultazione della documentazione istituzionale.

3. L'Archivio è articolato in sezioni coordinate:
   a. archivio istituzionale;
   b. archivio normativo e regolamentare;
   c. archivio amministrativo;
   d. archivio economico e finanziario;
   e. archivio tecnico;
   f. archivio operativo;
   g. archivio dei registri;
   h. archivio storico;
   i. archivio digitale;
   j. archivio delle evidenze e delle verifiche.
4. Le sezioni devono mantenere collegamenti documentali reciproci.

Art. 6 – Articolazione temporale degli archivi

1. L'Archivio è organizzato secondo tre livelli temporali.

A. Archivio corrente

Contiene la documentazione utilizzata nelle attività istituzionali e operative in corso.

B. Archivio di deposito

Contiene la documentazione non più utilizzata quotidianamente, ma ancora necessaria per esigenze amministrative, organizzative, tecniche o di verifica.

C. Archivio storico

Contiene la documentazione destinata alla conservazione permanente per il suo valore istituzionale, storico, organizzativo o documentale.

2. Il trasferimento tra le sezioni deve essere registrato.
3. Nessun trasferimento comporta automaticamente la perdita dell'identificazione originaria.

Art. 7 – Fascicolo documentale

1. La documentazione relativa a un medesimo procedimento, attività, progetto o funzione deve essere organizzata, ove opportuno, in fascicoli.
2. Ogni fascicolo deve riportare:
   a. codice identificativo;
   b. denominazione;
   c. settore di appartenenza;
   d. responsabile;
   e. data di apertura;
   f. documenti contenuti;
   g. stato;
   h. data di chiusura, ove applicabile;
   i. livello di accesso.
3. I fascicoli devono consentire la ricostruzione completa delle attività documentate.

Art. 8 – Registro generale dell'archivio

1. È istituito il Registro Generale dell'Archivio SIPSE (RGA-SIPSE).
2. Il Registro costituisce l'indice generale della documentazione conservata.
3. Per ciascun documento sono registrati:
   a. codice documentale;
   b. titolo;
   c. categoria;
   d. sistema di appartenenza;
   e. versione;
   f. data di emissione;
   g. data di archiviazione;
   h. collocazione;
   i. formato;
   j. livello di accesso;
   k. responsabile;
   l. stato di conservazione.
4. Il Registro deve essere aggiornato in occasione di ogni operazione archivistica rilevante.

TITOLO III – CONSERVAZIONE DEI DOCUMENTI

Art. 9 – Conservazione degli originali

1. Ogni documento ufficiale deve essere conservato nella versione originale o nella versione formalmente approvata, secondo la sua natura e il procedimento di formazione.
2. Per i documenti digitali deve essere preservato il file originale ricevuto o prodotto.
3. Per i documenti cartacei deve essere preservato il supporto originale, ove previsto e necessario.
4. Non è consentito sostituire un originale con una versione modificata senza conservarne la storia documentale.

Art. 10 – Conservazione delle copie

1. Le copie sono identificate in relazione alla loro funzione.
2. Sono distinte:
   a. copie di consultazione;
   b. copie operative;
   c. copie di sicurezza;
   d. copie di distribuzione;
   e. copie di lavoro;
   f. copie storiche.
3. Le copie devono essere riconducibili al documento di origine.
4. Le copie di lavoro non possono essere presentate come versioni ufficiali approvate.

Art. 11 – Conservazione delle versioni precedenti

1. Le versioni sostituite devono essere conservate secondo il piano di conservazione documentale.
2. Ogni versione precedente deve mantenere:
   a. il codice identificativo;
   b. il numero di versione;
   c. la data;
   d. lo stato storico;
   e. il collegamento alla versione successiva.
3. Le versioni precedenti devono essere chiaramente distinte dai documenti attualmente applicabili.
4. La conservazione storica deve impedire la confusione tra disposizioni precedenti e disposizioni aggiornate.

Art. 12 – Documentazione amministrativa e finanziaria

1. La documentazione amministrativa e finanziaria è conservata secondo criteri di integrità, riservatezza e reperibilità.
2. Sono comprese:
   a. registrazioni contabili;
   b. rendicontazioni;
   c. prospetti economici;
   d. documentazione bancaria;
   e. evidenze delle transazioni;
   f. documenti contrattuali;
   g. documentazione relativa alle operazioni finanziarie.
3. La conservazione deve rispettare gli obblighi applicabili alla natura dei documenti e dei soggetti coinvolti.
4. L'accesso è limitato ai soggetti autorizzati.

TITOLO IV – CONSERVAZIONE DIGITALE E PROTEZIONE TECNICA

Art. 13 – Archivio digitale

1. È istituito l'Archivio Digitale SIPSE (ADS-DIG).
2. L'Archivio Digitale costituisce la componente informatica del sistema documentale.
3. Deve consentire:
   a. acquisizione dei documenti;
   b. registrazione dei metadati;
   c. classificazione;
   d. indicizzazione;
   e. consultazione;
   f. controllo delle versioni;
   g. registrazione degli accessi;
   h. gestione delle copie;
   i. esportazione dei documenti;
   j. recupero delle informazioni.
4. L'archivio deve utilizzare sistemi di protezione adeguati alla criticità delle informazioni.

Art. 14 – Formati documentali

1. I documenti devono essere conservati in formati che assicurino leggibilità, disponibilità e possibilità di consultazione nel tempo.
2. Sono ammessi, secondo la natura del contenuto:
   a. PDF;
   b. PDF/A, ove appropriato;
   c. DOCX;
   d. XLSX;
   e. CSV;
   f. XML;
   g. JSON;
   h. PNG;
   i. JPEG;
   j. TIFF;
   k. formati tecnici specifici.
3. Per i documenti destinati alla conservazione a lungo termine devono essere preferiti formati documentati e ampiamente supportati.
4. La conversione di formato deve essere registrata quando può incidere sulle caratteristiche del documento.

Art. 15 – Metadati di conservazione

1. Ogni documento digitale deve essere associato a metadati adeguati.
2. I metadati comprendono almeno:
   a. identificativo;
   b. titolo;
   c. autore o funzione produttrice;
   d. data di formazione;
   e. data di registrazione;
   f. versione;
   g. formato;
   h. dimensione del file;
   i. classificazione;
   j. livello di accesso;
   k. impronta digitale, ove prevista;
   l. informazioni sulla conservazione;
   m. cronologia delle operazioni.
3. I metadati devono essere protetti contro modifiche non autorizzate.

Art. 16 – Impronta crittografica

1. Per i documenti digitali di particolare rilevanza può essere generata un'impronta crittografica mediante algoritmo SHA-256.
2. L'impronta è calcolata sul contenuto esatto del file.
3. Il valore generato è registrato insieme ai metadati del documento.
4. Ogni modifica del file determina un'impronta differente.
5. La verifica periodica consente di rilevare eventuali alterazioni rispetto al valore originariamente registrato.

6. L'impronta crittografica non sostituisce la firma elettronica, la marcatura temporale o le altre attestazioni eventualmente necessarie.

Art. 17 – Registrazione delle operazioni

1. Le operazioni significative sull'archivio digitale devono essere registrate.
2. Sono registrate, ove tecnicamente possibile:
   a. acquisizione;
   b. registrazione;
   c. consultazione;
   d. modifica dei metadati;
   e. trasferimento;
   f. esportazione;
   g. sostituzione;
   h. ripristino;
   i. cancellazione autorizzata.
3. Ogni registrazione deve indicare data, operazione e identificativo dell'utente o del sistema responsabile.
4. I registri delle operazioni devono essere protetti da alterazioni non autorizzate.

TITOLO V – BACKUP, RIPRISTINO E CONTINUITÀ

Art. 18 – Sistema di backup

1. È istituito il Sistema di Backup Documentale SIPSE (SBDS).
2. Il sistema protegge i documenti digitali contro perdita, danneggiamento, indisponibilità e incidenti informatici.
3. Le copie di sicurezza devono essere realizzate secondo un piano documentato.
4. Il piano deve indicare:
   a. sistemi interessati;
   b. dati e documenti inclusi;
   c. frequenza;
   d. destinazione;
   e. responsabile;
   f. modalità di verifica;
   g. tempi di conservazione delle copie;
   h. modalità di ripristino.

Art. 19 – Strategia di backup

1. La strategia di backup deve considerare:
   a. copie periodiche;
   b. copie incrementali o complete;
   c. copie separate dai sistemi principali;
   d. protezione da ransomware;
   e. controllo degli accessi;
   f. verifica della recuperabilità.

2. È raccomandata l'adozione di una strategia di protezione basata sul principio 3-2-1:
    - almeno tre copie dei dati;
    - almeno due supporti o sistemi differenti;
    - almeno una copia separata dalla sede o dall'ambiente operativo principale.
3. Per i documenti di maggiore criticità può essere adottata una copia non modificabile per un periodo definito.
4. La strategia deve essere proporzionata al rischio e alle risorse disponibili.

Art. 20 – Verifica delle copie di sicurezza

1. Le copie di sicurezza devono essere sottoposte a verifiche periodiche.
2. Le verifiche comprendono:
   a. completezza;
   b. leggibilità;
   c. integrità;
   d. disponibilità;
   e. possibilità di ripristino.
3. L'esito deve essere registrato nel Registro delle Verifiche e del Monitoraggio (RVM-MSP).
4. Le anomalie rilevate sono gestite attraverso il Registro delle Non Conformità (RNC-MSP).

Art. 21 – Ripristino documentale

1. In caso di perdita, danneggiamento o indisponibilità dei documenti, deve essere attivata la procedura di ripristino.
2. La procedura comprende:
   a. identificazione dell'incidente;
   b. valutazione dei documenti interessati;
   c. individuazione della copia disponibile;
   d. verifica dell'integrità;
   e. ripristino;
   f. controllo della completezza;
   g. registrazione dell'intervento.
3. Il ripristino deve preservare, per quanto possibile, le versioni e i metadati originari.
4. Gli incidenti significativi devono essere sottoposti a valutazione delle cause e ad eventuali azioni correttive.

Art. 22 – Continuità archivistica

1. Il sistema deve assicurare la continuità della disponibilità documentale anche in presenza di interruzioni operative.
2. Devono essere individuate le categorie documentali essenziali.
3. Per le categorie essenziali devono essere definite priorità di recupero.
4. La continuità archivistica è coordinata con il sistema MSP di gestione dei rischi e della resilienza.

TITOLO VI – ACCESSO E PROTEZIONE DELLE INFORMAZIONI

Art. 23 – Classificazione degli accessi

1. La documentazione è classificata secondo i seguenti livelli:

PUBBLICO: documentazione autorizzata alla consultazione generale.

ISTITUZIONALE: documentazione destinata alle strutture e ai soggetti autorizzati.

RISERVATO: documentazione contenente informazioni la cui divulgazione deve essere limitata.

ACCESSO LIMITATO: documentazione accessibile esclusivamente a soggetti specificamente autorizzati.

2. Il livello di accesso è attribuito in relazione al contenuto e alla finalità del documento.

Art. 24 – Autorizzazione e controllo degli accessi

1. L'accesso agli archivi è subordinato a specifiche autorizzazioni.
2. Le autorizzazioni devono essere attribuite secondo il principio del privilegio minimo.
3. Devono essere definite:
   a. identità dell'utilizzatore;
   b. funzione;
   c. livello di autorizzazione;
   d. ambito documentale;
   e. durata dell'autorizzazione, ove applicabile.
4. Le autorizzazioni devono essere periodicamente verificate.
5. La revoca di un'autorizzazione deve essere registrata.

Art. 25 – Protezione dei dati

1. La conservazione deve rispettare la normativa applicabile in materia di protezione dei dati personali e riservatezza.
2. I dati personali devono essere trattati secondo finalità determinate e con misure di sicurezza adeguate.
3. Devono essere evitati accessi, comunicazioni e conservazioni non giustificati.
4. La documentazione contenente dati personali deve essere soggetta a specifiche regole di accesso e conservazione.

Art. 26 – Protezione contro alterazioni e distruzioni

1. Devono essere adottate misure tecniche e organizzative contro:
   a. cancellazioni accidentali;
   b. alterazioni non autorizzate;
   c. accessi abusivi;
   d. malware;
   e. ransomware;
   f. perdita di supporti;
   g. danneggiamento fisico;
   h. indisponibilità dei servizi.
2. Le misure adottate devono essere proporzionate alla criticità documentale.

3. Gli incidenti devono essere registrati e gestiti secondo le procedure di sicurezza applicabili.

TITOLO VII – TEMPI DI CONSERVAZIONE E DISMISSIONE

Art. 27 – Piano di conservazione

1. È istituito il Piano di Conservazione Documentale SIPSE (PCD-SIPSE).
2. Il Piano stabilisce i tempi di conservazione in relazione alla natura e alla rilevanza dei documenti.
3. La determinazione dei tempi considera:
   a. valore istituzionale;
   b. valore amministrativo;
   c. valore contabile;
   d. rilevanza contrattuale;
   e. obblighi normativi;
   f. esigenze di audit;
   g. necessità di tutela dei diritti;
   h. valore storico.
4. I tempi di conservazione devono essere definiti prima di procedere a eventuali operazioni di scarto.

Art. 28 – Documenti destinati alla conservazione permanente

1. Sono candidati alla conservazione permanente, secondo il piano approvato:
   a. atti istitutivi;
   b. statuti;
   c. regolamenti fondamentali;
   d. deliberazioni di particolare rilevanza;
   e. atti di organizzazione;
   f. documenti relativi alla costituzione dei sistemi;
   g. registri istituzionali essenziali;
   h. documentazione storica;
   i. documentazione fondamentale relativa all'evoluzione del SIPSE.
2. La conservazione permanente deve essere accompagnata da adeguate misure di protezione e leggibilità.

Art. 29 – Scarto e dismissione

1. La cancellazione o lo scarto dei documenti sono consentiti esclusivamente secondo procedure formalizzate.
2. Prima dello scarto devono essere verificati:
   a. termine di conservazione;
   b. assenza di obblighi pendenti;
   c. assenza di contenziosi o verifiche in corso;
   d. autorizzazione del soggetto competente;
   e. assenza di interesse storico permanente.
3. Ogni operazione di scarto deve essere documentata.

4. La documentazione relativa allo scarto deve riportare:
   a. identificativi dei documenti;
   b. motivazione;
   c. data;
   d. soggetto autorizzante;
   e. modalità di eliminazione;
   f. esito dell'operazione.
5. La cancellazione non deve essere utilizzata per occultare anomalie, modifiche o responsabilità documentali.

TITOLO VIII – RESPONSABILITÀ E CONTROLLO

Art. 30 – Responsabile dell'Archivio Documentale

1. È individuata la funzione responsabile del coordinamento dell'Archivio Documentale SIPSE.
2. Essa assicura:
   a. organizzazione degli archivi;
   b. aggiornamento dei registri;
   c. classificazione;
   d. controllo delle collocazioni;
   e. coordinamento della conservazione;
   f. gestione delle richieste di consultazione;
   g. monitoraggio delle anomalie;
   h. coordinamento delle verifiche periodiche.
3. Le responsabilità devono essere attribuite formalmente.

Art. 31 – Responsabilità delle strutture

1. Le strutture produttrici sono responsabili della corretta formazione e trasmissione dei documenti all'archivio.
2. Devono garantire:
   a. identificazione;
   b. completezza;
   c. correttezza dei metadati;
   d. trasmissione delle versioni approvate;
   e. segnalazione delle anomalie;
   f. rispetto dei livelli di accesso.

Art. 32 – Verifica del sistema archivistico

1. Il sistema archivistico è sottoposto a verifiche periodiche.
2. Le verifiche riguardano:
   a. completezza degli archivi;
   b. reperibilità;
   c. integrità;
   d. disponibilità;

e. correttezza delle autorizzazioni;
f. esecuzione dei backup;
g. recuperabilità;
h. rispetto dei tempi di conservazione;
i. correttezza delle operazioni di scarto.

3. Gli esiti devono essere registrati.

Art. 33 – Indicatori di conservazione

1. Il sistema utilizza indicatori per misurare la qualità della conservazione.
2. Sono adottati almeno i seguenti indicatori:

- percentuale di documenti correttamente archiviati;
- percentuale di documenti con metadati completi;
- percentuale di documenti con identificativo univoco;
- percentuale di backup verificati;
- numero di anomalie di integrità;
- tempo medio di recupero documentale;
- numero di accessi non autorizzati rilevati;
- numero di documenti non reperibili;
- percentuale di revisioni correttamente registrate.

3. Gli indicatori sono aggiornati attraverso il sistema RVM-MSP.

TITOLO IX – INTEGRAZIONE CON IL SISTEMA DI MONITORAGGIO MSP

Art. 34 – Collegamento con RNC-MSP

1. Le anomalie relative alla conservazione e all'archiviazione sono registrate nel Registro delle Non Conformità.
2. Sono considerate anomalie, tra le altre:
   a. documenti mancanti;
   b. duplicazioni non controllate;
   c. alterazioni non autorizzate;
   d. errori di classificazione;
   e. perdita di metadati;
   f. mancata esecuzione dei backup;
   g. impossibilità di recupero.

Art. 35 – Collegamento con PAC-MSP

1. Le non conformità rilevate sono sottoposte a valutazione delle cause.
2. Quando necessario, è predisposto un Piano delle Azioni Correttive.
3. Le azioni possono comprendere:
   a. ripristino;
   b. recupero dei documenti;
   c. aggiornamento dei sistemi;

d. revisione delle autorizzazioni;
e. rafforzamento delle protezioni;
f. aggiornamento delle procedure.

Art. 36 – Collegamento con RVM-MSP e RMA-MSP

1. Il Registro delle Verifiche e del Monitoraggio raccoglie le evidenze dei controlli archivistici.
2. Il Registro delle Misure di Miglioramento raccoglie gli interventi destinati a incrementare la qualità e la resilienza della conservazione.
3. I quattro strumenti operativi MSP devono mantenere una relazione documentale tracciabile con l'Archivio.

TITOLO X – DISPOSIZIONI FINALI

Art. 37 – Coordinamento con gli atti precedenti

1. Il presente Regolamento costituisce attuazione degli indirizzi stabiliti dagli Atti n. 35/MSP e n. 36/MSP.
2. I tre atti costituiscono il primo nucleo coordinato del sistema documentale MSP:
   a. gestione documentale;
   b. codificazione e identificazione;
   c. conservazione e archiviazione.
3. Le disposizioni devono essere applicate congiuntamente.

Art. 38 – Attuazione operativa

1. L'attuazione del presente Regolamento è affidata alle funzioni formalmente individuate.
2. Devono essere predisposti:
   a. Registro Generale dell'Archivio;
   b. Piano di Conservazione Documentale;
   c. Registro delle Operazioni Archivistiche;
   d. Piano di Backup;
   e. Procedura di Ripristino;
   f. Registro delle Verifiche di Integrità;
   g. procedura di autorizzazione allo scarto.
3. Gli strumenti attuativi sono approvati secondo le competenze organizzative applicabili.

Art. 39 – Entrata in applicazione

1. Il presente Atto entra in applicazione a seguito della formale approvazione dell'organo competente.
2. La data di approvazione e la decorrenza sono registrate nel Registro Generale della Documentazione.

Art. 40 – Disposizione conclusiva

1. Il patrimonio documentale costituisce una componente essenziale della continuità organizzativa del SIPSE.

2. La sua conservazione deve assicurare la possibilità di ricostruire nel tempo l'evoluzione istituzionale, normativa, amministrativa, economica e operativa dei sistemi.
3. Nessun documento di rilevanza istituzionale può essere considerato adeguatamente conservato senza una identificazione riconoscibile, una collocazione documentata e misure proporzionate di protezione.

SIPSE – SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

MERCATO SOVRANO DEI POPOLI – MSP

ATTO N. 37/MSP

Regolamento di Conservazione, Archiviazione e Protezione del Patrimonio Documentale SIPSE–MSP.

Versione 1.0 – 18 novembre 2026.

Testo predisposto per l'approvazione dell'organo competente.