SIPSE

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

DPS-09

REGOLAMENTO DELLA SICUREZZA INFORMATICA, DELLA CONTINUITÀ OPERATIVA E DELLA PROTEZIONE DALLE INTERFERENZE

Disciplina internazionale della sicurezza digitale, della resilienza tecnologica, dell'integrità delle consultazioni e della protezione della volontà popolare

Codice: SIPSE-DPS-09
Atto di riferimento: Atto istitutivo SIPSE-DPS n. 18/2026
Sistema: SIPSE – Digital Participation System
Ambito: internazionale e transnazionale
Natura: regolamento tecnico, organizzativo, operativo e di sicurezza
Versione: 1.0 – 2026

Principio fondamentale:

La volontà dei popoli non può essere manipolata, alterata, soppressa o condizionata da alcuna interferenza tecnologica, economica, politica o organizzativa.

PREAMBOLO

Il Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE), nell'ambito dell'organizzazione e dello sviluppo del sistema di partecipazione democratica SIPSE-DPS,

considerato che:

- la sicurezza informatica costituisce una condizione essenziale per la protezione dei processi democratici digitali;
- la continuità delle consultazioni popolari rappresenta un elemento fondamentale per l'effettività della partecipazione;
- l'integrità dei dati, delle procedure e dei risultati deve essere protetta da accessi non autorizzati, alterazioni, manipolazioni e distruzioni;
- le infrastrutture digitali utilizzate per le consultazioni possono essere esposte ad attacchi informatici, sabotaggi, interruzioni e interferenze esterne;
- le consultazioni popolari permanenti richiedono un modello di sicurezza continuativo, non limitato al periodo di apertura del voto;

- la protezione della volontà popolare richiede la separazione funzionale tra identificazione, ammissione, espressione del voto, scrutinio e certificazione;
- nessun singolo soggetto deve poter disporre unilateralmente del controllo integrale del processo democratico;
- la sicurezza deve essere verificabile attraverso controlli indipendenti, registrazioni documentali e procedure di ripristino;

richiamati, per quanto applicabili:

1. Carta delle Nazioni Unite.
2. Dichiarazione universale dei diritti umani.
3. Patto internazionale sui diritti civili e politici.
4. Patto internazionale sui diritti economici, sociali e culturali.
5. Convenzione europea dei diritti dell'uomo.
6. Regolamento (UE) 2016/679.
7. Direttiva (UE) 2022/2555 – NIS2, nei casi di applicabilità.
8. Regolamento (UE) 2024/2847 – Cyber Resilience Act, nei casi di applicabilità.
9. Normativa nazionale ed europea sulla sicurezza delle reti, dei sistemi informativi e dei servizi digitali.

assunti come riferimenti tecnici:

- NIST Cybersecurity Framework 2.0;
- NIST Cybersecurity Framework Election Infrastructure Profile;
- standard ISO/IEC 27001 e ISO/IEC 27002;
- standard ISO 22301 per la continuità operativa;
- standard ISO/IEC 27035 per la gestione degli incidenti di sicurezza;
- linee guida ENISA sulla sicurezza delle infrastrutture elettorali;
- principi di sicurezza by design, privacy by design e zero trust.

adotta il seguente Regolamento.

TITOLO I – PRINCIPI GENERALI E OBIETTIVI

Articolo 1 – Oggetto

1. Il presente regolamento disciplina la sicurezza informatica, la protezione delle infrastrutture digitali, la continuità operativa e la prevenzione delle interferenze nel sistema SIPSE-DPS.
2. Sono disciplinati:

a. la sicurezza delle piattaforme;

b. la protezione delle consultazioni;

c. l'identificazione e l'autenticazione degli utenti;

d. la gestione degli accessi;

e. la crittografia;

f. la protezione dei dati;

g. la sicurezza dello scrutinio;

h. la prevenzione delle interferenze;

i. la gestione degli incidenti;

j. la continuità operativa;

k. il ripristino delle infrastrutture;

l. gli audit di sicurezza;

m. la responsabilità degli operatori.

Articolo 2 – Finalità

Il presente regolamento persegue le seguenti finalità:

1. Proteggere l'integrità delle consultazioni popolari.
2. Garantire la riservatezza delle preferenze individuali.
3. Prevenire accessi non autorizzati.
4. Impedire la manipolazione dei risultati.
5. Garantire la disponibilità delle piattaforme.
6. Proteggere i sistemi da attacchi informatici.
7. Assicurare la continuità dei servizi.
8. Prevenire interferenze politiche, economiche e tecnologiche.
9. Garantire la verificabilità indipendente.
10. Assicurare il ripristino delle attività dopo incidenti.
11. Proteggere l'autonomia delle consultazioni.
12. Rafforzare la fiducia dei popoli nel sistema.

Articolo 3 – Principio di Sovranità Digitale della Volontà Popolare

1. Il SIPSE riconosce la Sovranità Digitale della Volontà Popolare quale principio organizzativo fondamentale del SIPSE-DPS.
2. Tale principio consiste nella protezione dell'autenticità, dell'integrità, della libertà e della non manipolabilità della partecipazione democratica.
3. Nessun soggetto, interno o esterno, può disporre di poteri incontrollati sulle operazioni di partecipazione e scrutinio.
4. La volontà espressa dal partecipante deve essere protetta da qualsiasi alterazione, sostituzione, cancellazione o attribuzione indebita.
5. Ogni intervento tecnico deve essere tracciabile e verificabile.

Articolo 4 – Principi inderogabili di sicurezza

Il sistema si fonda sui seguenti principi:

a. sicurezza fin dalla progettazione;

b. protezione continua;

c. separazione delle funzioni;

d. minimo privilegio;

e. autenticazione forte;

f. indipendenza delle verifiche;

g. tracciabilità delle operazioni;

h. riservatezza dei dati;

i. resilienza delle infrastrutture;

j. ripristinabilità;

k. responsabilità individuale degli operatori;

l. verificabilità pubblica nei limiti della riservatezza.

Articolo 5 – Ambito di applicazione

Il regolamento si applica:

1. Alla piattaforma SIPSE-DPS.
2. Alle infrastrutture di elaborazione.
3. Ai sistemi di identificazione.
4. Ai sistemi di registrazione dei partecipanti.
5. Ai sistemi di voto.
6. Ai sistemi di scrutinio.
7. Ai sistemi di certificazione.
8. Ai registri documentali.
9. Alle infrastrutture di comunicazione.
10. Ai fornitori tecnologici.
11. Agli amministratori e agli operatori.
12. Ai soggetti esterni autorizzati.

TITOLO II – ARCHITETTURA DI SICUREZZA

Articolo 6 – Architettura modulare

1. Il SIPSE-DPS deve essere realizzato mediante un'architettura modulare.
2. Ogni componente deve avere una funzione definita, autorizzazioni limitate e responsabilità identificabili.
3. I moduli critici devono essere isolabili in caso di incidente.
4. L'architettura deve consentire la sostituzione o il ripristino di un componente senza compromettere l'intero sistema.

Articolo 7 – Separazione delle funzioni democratiche

Il sistema deve mantenere separati i seguenti livelli:

Livello 1 – Identificazione

Verifica dell'identità del partecipante attraverso procedure autorizzate.

Livello 2 – Abilitazione

Verifica del diritto di partecipazione alla specifica consultazione.

Livello 3 – Emissione del voto

Generazione e trasmissione della preferenza attraverso un canale protetto.

Livello 4 – Registrazione

Registrazione dell'avvenuta partecipazione senza esposizione della preferenza individuale.

Livello 5 – Scrutinio

Elaborazione delle preferenze attraverso procedure verificabili.

Livello 6 – Certificazione

Verifica indipendente e certificazione del risultato.

Livello 7 – Pubblicazione

Comunicazione dei risultati secondo il DPS-08.

Nessun amministratore ordinario deve poter controllare autonomamente tutti i livelli.

Articolo 8 – Isolamento delle infrastrutture

1. Le componenti di identificazione, voto, scrutinio e amministrazione devono essere separate logicamente e, per le componenti critiche, anche mediante segmentazione infrastrutturale.
2. Le comunicazioni tra i moduli devono utilizzare canali autenticati e protetti.
3. Gli accessi tra moduli devono essere autorizzati e registrati.
4. I sistemi amministrativi non devono avere accesso diretto alle preferenze individuali.

Articolo 9 – Principio Zero Trust

1. Nessun utente, dispositivo, servizio o componente è considerato affidabile per il solo fatto di appartenere alla rete interna.
2. Ogni accesso deve essere verificato in funzione dell'identità, del dispositivo, del contesto e delle autorizzazioni.
3. Le autorizzazioni devono essere limitate nel tempo e nello scopo.
4. Gli accessi privilegiati devono essere sottoposti a controlli rafforzati.

Articolo 10 – Ambiente di produzione e ambienti di prova

1. Gli ambienti di sviluppo, collaudo, formazione e produzione devono essere separati.
2. È vietato utilizzare dati reali di voto negli ambienti di prova, salvo specifiche procedure autorizzate e adeguatamente protette.
3. Gli aggiornamenti devono essere verificati prima della distribuzione nell'ambiente di produzione.
4. Ogni rilascio deve essere identificabile e reversibile secondo una procedura controllata.

TITOLO III – IDENTITÀ DIGITALE E AUTENTICAZIONE

Articolo 11 – Identificazione dei partecipanti

1. L'identificazione deve avvenire secondo procedure proporzionate al rischio e alle caratteristiche della consultazione.
2. Il sistema deve verificare che il soggetto richiedente sia effettivamente il partecipante autorizzato.
3. I dati identificativi devono essere trattati separatamente dai dati relativi alla preferenza.
4. Devono essere previste modalità alternative per i soggetti che non dispongano di strumenti digitali adeguati.

Articolo 12 – Autenticazione multifattore

1. Gli accessi alle funzioni amministrative e privilegiate devono essere protetti mediante autenticazione multifattore.
2. Per le funzioni ordinarie di partecipazione devono essere adottati meccanismi proporzionati al rischio e compatibili con la segretezza del voto.
3. Le credenziali compromesse devono poter essere revocate tempestivamente.
4. Gli amministratori devono utilizzare credenziali individuali e non condivise.

Articolo 13 – Gestione delle credenziali

1. Ogni utente autorizzato dispone di credenziali personali.
2. È vietata la condivisione delle credenziali.
3. Le credenziali devono essere protette attraverso sistemi crittografici adeguati.
4. Le procedure di recupero devono prevedere verifiche supplementari.
5. Le credenziali privilegiate devono essere conservate in sistemi dedicati e sottoposte a controllo.

Articolo 14 – Gestione delle sessioni

Il sistema deve:

a. limitare la durata delle sessioni;

b. interrompere le sessioni inattive secondo parametri di rischio;

c. impedire il riutilizzo improprio dei token;

d. proteggere le comunicazioni;

e. rilevare sessioni anomale;

f. consentire la revoca delle sessioni compromesse.

Articolo 15 – Autenticazione delle operazioni critiche

Le operazioni che incidono sull'integrità delle consultazioni devono richiedere autorizzazioni rafforzate.

Sono considerate critiche:

1. Apertura di una consultazione.
2. Modifica dei parametri.
3. Attivazione del sistema di voto.
4. Sospensione della consultazione.
5. Chiusura della votazione.
6. Avvio dello scrutinio.
7. Certificazione dei risultati.
8. Modifica delle configurazioni di sicurezza.
9. Aggiornamento delle componenti critiche.

TITOLO IV – CRITTOGRAFIA E PROTEZIONE DEL VOTO

Articolo 16 – Protezione crittografica

1. I dati sensibili devono essere protetti mediante tecniche crittografiche riconosciute e adeguate al rischio.
2. Le comunicazioni devono utilizzare protocolli sicuri aggiornati.
3. I dati conservati devono essere cifrati quando necessario.
4. Gli algoritmi e le implementazioni devono essere sottoposti a valutazione tecnica indipendente.
5. Le scelte crittografiche devono considerare l'evoluzione delle capacità computazionali e i rischi futuri.

Articolo 17 – Separazione tra identità e preferenza

1. Il sistema deve impedire il collegamento diretto tra identità del partecipante e voto espresso.
2. La registrazione dell'avvenuta partecipazione deve essere separata dalla registrazione della preferenza.
3. Devono essere adottate misure contro la correlazione temporale e statistica dei dati.
4. È vietata la conservazione di registri che consentano agli operatori ordinari di ricostruire il comportamento elettorale individuale.

Articolo 18 – Integrità del voto

1. Ogni voto validamente espresso deve essere protetto contro alterazioni, duplicazioni e cancellazioni.
2. Il sistema deve disporre di meccanismi di verifica dell'integrità della registrazione.
3. Le procedure di scrutinio devono poter essere controllate da soggetti indipendenti.
4. Nessuna modifica del voto può essere effettuata senza una procedura formalmente autorizzata e verificabile.

Articolo 19 – Crittografia avanzata e scrutinio verificabile

1. Il SIPSE-DPS può utilizzare tecniche crittografiche avanzate per garantire la riservatezza e la verificabilità delle operazioni.
2. Tra le tecniche valutabili rientrano:

a. crittografia omomorfica;

b. sistemi di voto verificabile end-to-end;

c. prove a conoscenza zero;

d. firme digitali;

e. registri crittografici append-only;

f. protocolli a condivisione della chiave;

g. sistemi di calcolo multiparte sicuro.

3. Le tecnologie possono essere adottate soltanto dopo una valutazione indipendente della sicurezza, della correttezza matematica e della concreta implementazione.
4. L'utilizzo di una tecnologia crittografica non costituisce, da solo, prova della correttezza dell'intera consultazione.

Articolo 20 – Gestione delle chiavi crittografiche

1. Le chiavi utilizzate nelle funzioni critiche devono essere sottoposte a procedure controllate di generazione, custodia, utilizzo, rotazione e revoca.
2. È vietato che un singolo amministratore disponga autonomamente di tutte le chiavi necessarie alle operazioni di scrutinio o certificazione.
3. Possono essere utilizzati sistemi di custodia distribuita e procedure di autorizzazione congiunta.
4. Le procedure di recupero devono essere documentate e verificate.
5. Le chiavi compromesse devono essere revocate e sostituite secondo procedure formalizzate.

Articolo 21 – Autorizzazione distribuita

1. Per le operazioni critiche può essere adottato un modello di autorizzazione distribuita.
2. Il modello può prevedere la partecipazione congiunta di più soggetti indipendenti.
3. Come architettura di riferimento può essere adottato un sistema di soglia, ad esempio 3 autorizzazioni su 5 soggetti distinti, previa valutazione del rischio.
4. La composizione dei soggetti autorizzati deve garantire indipendenza e separazione delle responsabilità.
5. Nessun soggetto può modificare unilateralmente le regole di autorizzazione.

Articolo 22 – Divieto di manipolazione del voto

È vietato:

a. modificare una preferenza;

b. inserire voti non espressi;

c. eliminare voti validamente registrati;

d. duplicare una partecipazione;

e. alterare il conteggio;

f. impedire selettivamente l'accesso al voto;

g. modificare i risultati pubblicati;

h. introdurre codice non autorizzato nei sistemi di scrutinio.

Ogni tentativo deve essere registrato e sottoposto a indagine.

TITOLO V – SICUREZZA DELLE INFRASTRUTTURE

Articolo 23 – Protezione delle reti

1. Le infrastrutture di rete devono essere protette da accessi non autorizzati.
2. Devono essere adottati sistemi di filtraggio, monitoraggio e rilevamento delle intrusioni.
3. Le reti critiche devono essere segmentate.
4. Gli accessi remoti devono essere autorizzati e protetti.
5. Le configurazioni devono essere periodicamente verificate.

Articolo 24 – Protezione dei server e delle piattaforme

Le infrastrutture devono prevedere:

a. sistemi operativi aggiornati;

b. protezione contro malware;

c. gestione delle vulnerabilità;

d. controllo delle configurazioni;

e. monitoraggio delle risorse;

f. protezione contro gli accessi abusivi;

g. sistemi di registrazione degli eventi;

h. procedure di ripristino.

Articolo 25 – Protezione contro gli attacchi DDoS

1. Il SIPSE-DPS deve predisporre misure di protezione contro gli attacchi di negazione distribuita del servizio.
2. Le misure possono includere:

a. filtraggio del traffico;

b. distribuzione controllata del carico;

c. sistemi di mitigazione DDoS;

d. infrastrutture ridondate;

e. protezione dei servizi DNS;

f. canali alternativi di comunicazione.

3. Gli attacchi non devono comportare la perdita o la duplicazione delle preferenze validamente registrate.

Articolo 26 – Sicurezza delle applicazioni

1. Le applicazioni devono essere sviluppate secondo principi di sicurezza by design.
2. Devono essere eseguite verifiche del codice e delle dipendenze.
3. Le vulnerabilità devono essere classificate in funzione della gravità.
4. Le componenti critiche devono essere sottoposte a test di sicurezza prima del rilascio.
5. Devono essere mantenute procedure di aggiornamento controllato.

Articolo 27 – Sicurezza della catena di fornitura

1. I fornitori tecnologici devono essere sottoposti a valutazione del rischio.
2. Devono essere verificati:

a. provenienza dei componenti;

b. integrità del software;

c. gestione delle vulnerabilità;

d. dipendenze tecnologiche;

e. accessi dei fornitori;

f. localizzazione e trattamento dei dati;

g. capacità di continuità operativa.

3. I contratti devono prevedere obblighi di sicurezza, comunicazione degli incidenti, audit e restituzione o cancellazione dei dati.
4. Il SIPSE deve evitare dipendenze tecnologiche che impediscano la continuità autonoma del servizio.

TITOLO VI – PROTEZIONE DALLE INTERFERENZE

Articolo 28 – Definizione di interferenza

Ai fini del presente regolamento costituisce interferenza qualsiasi attività diretta o indiretta a compromettere la libertà, l'autenticità, la disponibilità, l'integrità o la regolarità di una consultazione.

Le interferenze possono essere:

1. Informatiche.
2. Politiche.
3. Economiche.
4. Organizzative.
5. Tecnologiche.
6. Informative.
7. Psicologiche o intimidatorie.
8. Provenienti da soggetti interni o esterni.

Articolo 29 – Interferenze informatiche

Sono considerate interferenze informatiche:

a. accessi abusivi;

b. furto di credenziali;

c. introduzione di codice malevolo;

d. alterazione dei registri;

e. manipolazione dei dati;

f. attacchi ai server;

g. interruzione intenzionale dei servizi;

h. compromissione delle chiavi crittografiche;

i. attacchi alla catena di fornitura.

Articolo 30 – Interferenze politiche ed economiche

1. È vietato utilizzare risorse economiche o poteri organizzativi per condizionare le operazioni tecniche della consultazione.
2. È vietata qualsiasi pressione esercitata sugli operatori per modificare procedure o risultati.
3. I finanziatori non possono ottenere accesso privilegiato alle infrastrutture.
4. I soggetti promotori non possono modificare unilateralmente i sistemi di scrutinio.
5. Ogni tentativo di interferenza deve essere registrato.

Articolo 31 – Manipolazione informativa e interferenze ibride

1. Il SIPSE-DPS adotta misure per rilevare e documentare campagne coordinate di manipolazione informativa che possano compromettere la regolarità delle consultazioni.
2. Sono oggetto di monitoraggio, nel rispetto della libertà di espressione:

a. falsificazione delle comunicazioni ufficiali;

b. impersonificazione degli organismi istituzionali;

c. diffusione di risultati fraudolenti;

d. campagne automatizzate coordinate dirette a compromettere i servizi;

e. utilizzo ingannevole di contenuti sintetici attribuiti falsamente al SIPSE;

f. tentativi di sottrazione o pubblicazione illecita di dati.

3. La semplice espressione di opinioni contrarie, critiche o dissenzienti non costituisce interferenza.
4. Il sistema non può essere utilizzato per censurare il dissenso politico.

Articolo 32 – Neutralità istituzionale

1. Gli strumenti di sicurezza non possono essere utilizzati per favorire una delle opzioni di voto.
2. Le misure devono essere neutrali rispetto al contenuto del quesito.
3. Le limitazioni all'accesso devono fondarsi su criteri tecnici e oggettivi.
4. Le decisioni di sospensione devono essere motivate e documentate.

TITOLO VII – MONITORAGGIO E RILEVAMENTO

Articolo 33 – Centro di sicurezza operativa

1. È istituito il Centro di Sicurezza Operativa SIPSE-DPS, denominato SIPSE-SOC.
2. Il Centro assicura il monitoraggio continuativo delle infrastrutture critiche.
3. Le sue funzioni comprendono:

a. monitoraggio degli eventi;

b. rilevamento delle anomalie;

c. analisi degli incidenti;

d. coordinamento degli interventi;

e. gestione delle segnalazioni;

f. produzione di rapporti tecnici;

g. supporto alla continuità operativa.

4. Il Centro opera in conformità alle autorizzazioni e alle competenze formalmente attribuite.

Articolo 34 – Monitoraggio permanente

1. Il monitoraggio deve essere attivo continuativamente per le infrastrutture critiche.
2. Devono essere rilevati accessi anomali, variazioni non autorizzate, guasti e comportamenti incompatibili con le configurazioni approvate.
3. I sistemi di monitoraggio devono essere protetti contro la manipolazione.
4. Gli eventi rilevanti devono essere registrati in archivi protetti.

Articolo 35 – Registro degli eventi di sicurezza

È istituito il Registro degli Eventi di Sicurezza, contenente:

1. Identificativo dell'evento.
2. Data e ora.
3. Componente interessato.
4. Tipologia di anomalia.
5. Gravità.
6. Responsabile della gestione.
7. Azioni intraprese.
8. Stato dell'incidente.
9. Esito della verifica.
10. Misure correttive.

Articolo 36 – Classificazione delle minacce

Le minacce sono classificate secondo quattro livelli:

Livello 1 – Basso

Anomalia limitata senza impatto sui servizi critici.

Livello 2 – Moderato

Incidente con impatto circoscritto e contenibile.

Livello 3 – Alto

Compromissione significativa di un servizio o di una componente essenziale.

Livello 4 – Critico

Compromissione effettiva o altamente probabile dell'integrità, della riservatezza o della disponibilità di una consultazione.

La classificazione può essere aggiornata in seguito all'evoluzione dell'incidente.

TITOLO VIII – GESTIONE DEGLI INCIDENTI

Articolo 37 – Obbligo di segnalazione

1. Ogni operatore che rilevi un incidente deve segnalarlo tempestivamente al SIPSE-SOC.
2. I fornitori devono comunicare gli incidenti secondo i termini contrattuali e gli obblighi normativi applicabili.
3. La segnalazione deve contenere le informazioni disponibili e non deve essere ritardata in attesa di una ricostruzione completa.

Articolo 38 – Procedura di risposta

La gestione degli incidenti si articola nelle seguenti fasi:

1. Rilevamento.
2. Registrazione.
3. Classificazione.
4. Contenimento.
5. Analisi.
6. Eradicazione della causa.
7. Ripristino.
8. Verifica dell'integrità.
9. Comunicazione.
10. Relazione conclusiva.

Articolo 39 – Unità di risposta agli incidenti

1. È istituita l'unità di risposta agli incidenti SIPSE-DPS, denominata SIPSE-CSIRT.
2. L'unità coordina le attività tecniche di risposta.
3. Può richiedere l'intervento di specialisti esterni indipendenti.
4. Deve conservare la documentazione delle attività svolte.
5. Non può certificare autonomamente la regolarità di un sistema sul quale abbia effettuato interventi critici senza una verifica indipendente successiva.

Articolo 40 – Sospensione cautelativa

1. In presenza di un incidente che possa compromettere l'integrità di una consultazione, il responsabile della sicurezza può proporre la sospensione cautelativa delle operazioni interessate.
2. La sospensione deve essere proporzionata al rischio.
3. Deve essere documentata e comunicata ai soggetti interessati.
4. Non può comportare la cancellazione delle partecipazioni validamente registrate.
5. La ripresa richiede una verifica dell'integrità del sistema e un'autorizzazione formalizzata.

Articolo 41 – Comunicazione degli incidenti

1. Gli incidenti rilevanti devono essere comunicati agli organi competenti.
2. Le comunicazioni devono distinguere tra informazioni confermate, valutazioni preliminari e ipotesi investigative.
3. Quando richiesto, sono effettuate notifiche alle autorità competenti e agli interessati secondo la normativa applicabile.
4. Il DPS-08 disciplina la pubblicazione delle informazioni destinate al pubblico.

Articolo 42 – Rapporto post-incidente

Ogni incidente di livello alto o critico deve produrre un rapporto contenente:

a. descrizione dell'evento;

b. cronologia;

c. sistemi coinvolti;

d. impatto sulla consultazione;

e. dati eventualmente compromessi;

f. misure di contenimento;

g. esito delle verifiche;

h. misure correttive;

i. valutazione del rischio residuo;

j. raccomandazioni preventive.

TITOLO IX – CONTINUITÀ OPERATIVA E RESILIENZA

Articolo 43 – Piano di continuità operativa

1. Il SIPSE deve predisporre un Piano di Continuità Operativa, denominato SIPSE-BCP.
2. Il Piano disciplina la prosecuzione delle attività in presenza di:

a. attacchi informatici;

b. guasti infrastrutturali;

c. interruzioni di rete;

d. indisponibilità dei fornitori;

e. calamità naturali;

f. emergenze energetiche;

g. perdita di disponibilità dei sistemi;

h. incidenti che coinvolgano il personale.

3. Il Piano deve essere aggiornato periodicamente.

Articolo 44 – Piano di ripristino

1. È predisposto un Piano di Disaster Recovery, denominato SIPSE-DRP.
2. Il Piano deve prevedere:

a. sistemi di riserva;

b. copie di sicurezza;

c. infrastrutture alternative;

d. procedure di ripristino;

e. verifica dell'integrità;

f. responsabilità operative;

g. comunicazioni di emergenza.

3. I sistemi di ripristino devono essere protetti contro la compromissione simultanea dei sistemi principali.

Articolo 45 – Obiettivi di ripristino

Il SIPSE adotta i seguenti obiettivi iniziali di riferimento, da convalidare attraverso un'analisi d'impatto operativo.

Parametro	Obiettivo proposto
RTO – servizi critici	4 ore
RTO – servizi secondari	24 ore
RPO – registri operativi	15 minuti
RPO – archivi documentali	24 ore
Disponibilità annuale dei servizi critici	99,95%

1. Gli obiettivi indicano livelli progettuali e non costituiscono garanzie assolute.
2. Il RTO identifica il tempo massimo obiettivo per il ripristino.
3. Il RPO identifica la quantità massima obiettivo di dati che può andare perduta in un incidente.

4. Per i dati relativi alle preferenze validamente registrate devono essere adottate misure specifiche affinché il ripristino non produca cancellazioni, duplicazioni o alterazioni.

Articolo 46 – Ridondanza

1. Le componenti critiche devono disporre di meccanismi di ridondanza.
2. Le copie di sicurezza devono essere conservate in ambienti separati.
3. Le infrastrutture alternative devono essere sottoposte a verifiche periodiche.
4. La ridondanza non deve creare ulteriori possibilità di accesso non autorizzato.

Articolo 47 – Backup e conservazione

1. Devono essere effettuate copie di sicurezza periodiche.
2. Le copie devono essere protette da cifratura e controlli di accesso.
3. Devono essere previste copie isolate o immutabili per le componenti critiche.
4. Il ripristino deve essere testato.
5. I backup non devono essere considerati validi prima della verifica della loro integrità.

Articolo 48 – Continuità delle consultazioni permanenti

1. Le consultazioni permanenti devono disporre di procedure specifiche per la gestione delle interruzioni.
2. In caso di indisponibilità, il sistema deve conservare lo stato verificabile della consultazione.
3. La sospensione non deve alterare i voti validamente registrati.
4. La ripresa deve avvenire dopo la verifica dell'integrità delle registrazioni.
5. La durata della sospensione deve essere comunicata pubblicamente.
6. Quando la continuità non può essere garantita senza compromettere le garanzie democratiche, la consultazione deve essere sospesa.

Articolo 49 – Canali alternativi

Il SIPSE può predisporre modalità alternative di partecipazione, nei limiti del regolamento specifico della consultazione.

Le modalità alternative devono garantire:

a. unicità della partecipazione;

b. equivalenza delle garanzie;

c. protezione della segretezza;

d. tracciabilità amministrativa;

e. verificabilità dello scrutinio.

Non è ammessa l'attivazione di un canale alternativo che consenta duplicazioni o alterazioni delle preferenze.

TITOLO X – SICUREZZA DELLE CONSULTAZIONI PERMANENTI

Articolo 50 – Protezione del ciclo democratico

1. La sicurezza deve essere garantita durante tutte le fasi della consultazione.
2. Il sistema deve proteggere:

a. registrazione degli aventi diritto;

b. ammissione;

c. apertura;

d. espressione del voto;

e. registrazione;

f. scrutinio;

g. certificazione;

h. pubblicazione;

i. archiviazione.

Articolo 51 – Verifica preventiva

Prima dell'apertura di una consultazione devono essere eseguiti:

1. Controllo delle configurazioni.
2. Verifica delle credenziali privilegiate.
3. Verifica dei sistemi crittografici.
4. Controllo delle autorizzazioni.
5. Test di disponibilità.
6. Verifica dei backup.
7. Controllo dell'integrità del software.
8. Verifica dei canali di comunicazione.
9. Controllo della separazione dei dati.
10. Approvazione del responsabile della sicurezza.

Articolo 52 – Integrità durante il voto

1. Il sistema deve monitorare continuamente le componenti coinvolte nella consultazione.
2. Ogni variazione non autorizzata deve generare un evento di sicurezza.

3. Devono essere adottate misure contro la manipolazione automatizzata delle partecipazioni.
4. Le anomalie devono essere analizzate senza compromettere la libertà di voto.
5. Nessun meccanismo di controllo può esporre la preferenza individuale.

Articolo 53 – Chiusura e scrutinio

1. La chiusura della consultazione deve essere eseguita secondo procedure formalizzate.
2. L'avvio dello scrutinio deve richiedere le autorizzazioni previste.
3. Le operazioni devono essere documentate.
4. Le verifiche devono consentire di accertare la corrispondenza tra le registrazioni valide e il risultato.
5. Il risultato non può essere dichiarato certificato prima del completamento dei controlli previsti.

Articolo 54 – Certificazione dell'integrità

1. La certificazione deve essere affidata a soggetti distinti da quelli responsabili della gestione ordinaria della piattaforma.
2. Il certificatore deve verificare almeno:

a. integrità delle registrazioni;

b. regolarità dello scrutinio;

c. correttezza dei conteggi;

d. rispetto delle procedure;

e. assenza di anomalie non risolte che possano compromettere il risultato.

3. Le eventuali riserve devono essere esplicitate.
4. Il certificato deve essere pubblicato secondo il DPS-08.

TITOLO XI – AUDIT, VERIFICHE E TEST DI SICUREZZA

Articolo 55 – Audit indipendente

1. Il SIPSE-DPS è sottoposto ad audit periodici.
2. Gli audit devono comprendere aspetti organizzativi, tecnologici, documentali e procedurali.
3. I verificatori devono essere indipendenti dalle attività sottoposte a controllo.
4. Gli audit devono produrre rapporti documentati.

Articolo 56 – Test di vulnerabilità

1. Devono essere eseguite verifiche periodiche delle vulnerabilità.
2. Le componenti critiche devono essere sottoposte a test approfonditi prima dell'utilizzo e dopo modifiche sostanziali.
3. I test devono essere autorizzati e condotti in ambienti controllati.
4. I risultati devono essere classificati secondo gravità e rischio.

Articolo 57 – Test di penetrazione

1. Il SIPSE può autorizzare test di penetrazione effettuati da professionisti qualificati e indipendenti.
2. I test devono essere preceduti da un piano di attività.
3. Devono essere stabiliti limiti operativi per evitare danni ai sistemi.
4. Le vulnerabilità individuate devono essere registrate e corrette.
5. Il rapporto conclusivo deve essere conservato e sottoposto a verifica.

Articolo 58 – Simulazioni di emergenza

1. Il SIPSE organizza almeno una simulazione annuale di incidente informatico critico.
2. Le simulazioni possono comprendere:

a. indisponibilità della piattaforma;

b. attacco DDoS;

c. compromissione delle credenziali;

d. perdita di un'infrastruttura;

e. indisponibilità del fornitore;

f. sospetto di alterazione dei dati;

g. compromissione di una componente di scrutinio.

3. I risultati sono utilizzati per aggiornare il BCP e il DRP.

TITOLO XII – GOVERNANCE E RESPONSABILITÀ

Articolo 59 – Organi della sicurezza

Sono istituiti:

1. Comitato di Sicurezza Digitale.
2. Direzione della Sicurezza Informatica.

3. Centro di Sicurezza Operativa SIPSE-SOC.
4. Unità di risposta agli incidenti SIPSE-CSIRT.
5. Responsabile della Continuità Operativa.
6. Responsabile della Protezione dei Dati, ove richiesto.
7. Organismo indipendente di audit.

Articolo 60 – Comitato di Sicurezza Digitale

Il Comitato:

a. approva gli indirizzi generali di sicurezza;

b. valuta i rischi strategici;

c. approva i piani di continuità;

d. esamina gli incidenti critici;

e. verifica l'attuazione delle misure correttive;

f. promuove la formazione;

g. riferisce agli organi competenti del SIPSE.

Articolo 61 – Direzione della Sicurezza Informatica

La Direzione:

1. attua le politiche di sicurezza;
2. coordina le attività tecniche;
3. gestisce le autorizzazioni;
4. supervisiona il monitoraggio;
5. gestisce le vulnerabilità;
6. coordina gli interventi;
7. mantiene la documentazione;
8. presenta rapporti periodici.

Articolo 62 – Separazione dei poteri

1. La gestione tecnica non può coincidere integralmente con la verifica indipendente.
2. Il gestore della piattaforma non può certificare da solo il risultato delle consultazioni.
3. Il responsabile finanziario non può modificare le configurazioni di voto.
4. Il promotore della consultazione non può intervenire unilateralmente nello scrutinio.
5. Le funzioni critiche devono essere distribuite secondo criteri di indipendenza e controllo reciproco.

Articolo 63 – Responsabilità dei fornitori

1. I fornitori devono rispettare le politiche di sicurezza del SIPSE.

2. Devono segnalare tempestivamente le vulnerabilità e gli incidenti rilevanti.
3. Devono consentire le verifiche previste dal contratto.
4. Non possono utilizzare dati o infrastrutture per finalità diverse da quelle autorizzate.
5. Alla cessazione del rapporto devono restituire o cancellare i dati secondo le istruzioni e gli obblighi applicabili.

Articolo 64 – Formazione e qualificazione

1. Gli operatori devono ricevere formazione periodica.
2. Gli amministratori delle infrastrutture critiche devono possedere competenze adeguate.
3. Gli addetti alla sicurezza devono essere sottoposti a programmi di aggiornamento.
4. La formazione deve comprendere:

a. sicurezza informatica;

b. protezione dei dati;

c. gestione degli incidenti;

d. sicurezza delle consultazioni;

e. continuità operativa;

f. prevenzione delle interferenze;

g. responsabilità istituzionale.

TITOLO XIII – COOPERAZIONE E STANDARD INTERNAZIONALI

Articolo 65 – Cooperazione tecnica

Il SIPSE può promuovere accordi di cooperazione con:

a. università;

b. centri di ricerca;

c. laboratori di sicurezza informatica;

d. organismi di certificazione;

e. organizzazioni internazionali;

f. istituzioni di cybersicurezza;

g. fornitori tecnologici qualificati.

Articolo 66 – Adozione degli standard

1. Il SIPSE promuove l'adozione progressiva degli standard internazionali pertinenti.
2. L'adozione deve essere documentata e verificabile.
3. Il rispetto di uno standard deve essere comprovato attraverso verifiche appropriate.
4. Nessuna dichiarazione di conformità può essere rilasciata senza evidenze documentali.

Articolo 67 – Evoluzione tecnologica

1. Il SIPSE deve monitorare l'evoluzione delle tecnologie e delle minacce.
2. Particolare attenzione è riservata a:

a. intelligenza artificiale;

b. attacchi automatizzati;

c. crittografia post-quantistica;

d. identità digitali;

e. sistemi distribuiti;

f. nuove vulnerabilità infrastrutturali.

3. Gli aggiornamenti devono essere sottoposti a valutazione del rischio.
4. Le tecnologie emergenti non possono essere adottate nelle funzioni critiche senza verifica indipendente.

TITOLO XIV – VIOLAZIONI, MISURE CORRETTIVE E GARANZIE

Articolo 68 – Violazioni

Costituiscono violazioni:

1. Accesso abusivo.
2. Manipolazione dei dati.
3. Alterazione delle preferenze.
4. Divulgazione di informazioni riservate.
5. Utilizzo improprio delle credenziali.
6. Disattivazione non autorizzata dei controlli.
7. Cancellazione dei registri.
8. Compromissione intenzionale della continuità.

9. Occultamento di incidenti.
10. Falsificazione delle certificazioni.

Articolo 69 – Misure correttive

In presenza di violazioni possono essere adottate:

a. revoca delle autorizzazioni;

b. sospensione degli accessi;

c. isolamento delle componenti compromesse;

d. ripristino dei sistemi;

e. audit straordinari;

f. revisione delle procedure;

g. risoluzione dei rapporti contrattuali, ove prevista;

h. segnalazione alle autorità competenti.

Articolo 70 – Protezione dei segnalanti

1. È istituito un canale riservato per la segnalazione di vulnerabilità e violazioni.
2. Le segnalazioni devono essere trattate con riservatezza.
3. È vietata ogni ritorsione nei confronti dei segnalanti in buona fede.
4. Le vulnerabilità devono essere gestite attraverso procedure di divulgazione coordinata e responsabile.

Articolo 71 – Salvaguardia dei diritti fondamentali

1. Le misure di sicurezza devono rispettare i diritti fondamentali.
2. Il monitoraggio non può trasformarsi in sorveglianza indiscriminata dei partecipanti.
3. Le misure di prevenzione non possono essere utilizzate per discriminare o limitare il dissenso.
4. La sicurezza deve essere proporzionata al rischio e alle finalità legittime.

TITOLO XV – DISPOSIZIONI FINALI

Articolo 72 – Coordinamento normativo

Il presente regolamento è coordinato con:

1. DPS-01 – Regolamento generale del sistema.

2. DPS-02 – Regolamento della Consultazione Popolare Permanente.
3. DPS-03 – Regolamento economico, tariffario e dei servizi.
4. DPS-04 – Regolamento dei controlli, delle verifiche e delle certificazioni.
5. DPS-05 – Contratto internazionale standard.
6. DPS-06 – Manuale operativo generale del SIPSE-DPS.
7. DPS-07 – Regolamento del Fondo per la Partecipazione dei Popoli.
8. DPS-08 – Regolamento della Trasparenza, della Pubblicità e dell'Accesso ai Dati.

Articolo 73 – Prevalenza delle norme applicabili

1. Il presente regolamento deve essere interpretato in conformità alle norme imperative e alle disposizioni legislative applicabili.
2. In caso di conflitto, prevalgono le disposizioni inderogabili dell'ordinamento competente.
3. Gli obblighi di notifica, cooperazione e comunicazione alle autorità competenti rimangono impregiudicati.

Articolo 74 – Revisione periodica

1. Il presente regolamento è sottoposto a revisione almeno ogni dodici mesi.
2. La revisione può essere anticipata in caso di incidenti critici, vulnerabilità sistemiche o innovazioni tecnologiche.
3. Ogni aggiornamento deve essere documentato e pubblicato secondo il DPS-08.

Articolo 75 – Entrata in vigore

Il presente regolamento entra in vigore dalla data della sua approvazione e pubblicazione da parte degli organi competenti del SIPSE.

DISPOSIZIONE ISTITUZIONALE CONCLUSIVA

Il SIPSE riconosce che la protezione della volontà popolare costituisce una responsabilità tecnica, organizzativa e istituzionale permanente.

La sicurezza del SIPSE-DPS non deve essere affidata alla fiducia in un singolo amministratore, in un fornitore tecnologico o in un organismo di controllo.

Deve essere il risultato di un sistema articolato di garanzie, separazioni funzionali, verifiche indipendenti e responsabilità documentate.

Nessuna infrastruttura può essere considerata invulnerabile. Per questo motivo il SIPSE adotta un modello fondato sulla prevenzione, sul rilevamento, sulla risposta, sul ripristino e sulla verifica.

La continuità tecnologica non deve mai prevalere sull'integrità democratica: quando non è possibile garantire la sicurezza di una consultazione, la sospensione controllata rappresenta una misura di tutela della volontà popolare.

La tecnologia deve servire i popoli, non governarli.

La sicurezza deve proteggere il voto, non controllarlo.

La sovranità digitale deve appartenere alla volontà dei partecipanti, non a chi gestisce l'infrastruttura.

SIPSE – Sistema delle Istituzioni dei Popoli per la Sovranità Economica

Il voto appartiene ai popoli.

La sicurezza appartiene alla democrazia.

La volontà popolare non è manipolabile.

PAX NON ABSENTIA BELLI SED PRAESENTIA IUSTITIAE.

Allegato tecnico A – Architettura di sicurezza SIPSE-DPS

La struttura operativa dovrà essere organizzata in sei livelli coordinati.

SIPSE Cybersecurity Architecture

Architettura funzionale proposta

01

GOVERNANCE

Politiche, responsabilità e gestione del rischio

02

IDENTITY & ACCESS

Identità, autenticazione e autorizzazioni

03

PROTECTION

Crittografia, isolamento e protezione delle reti

04

MONITORING

SIPSE-SOC, rilevamento e analisi delle anomalie

05

RESPONSE & RECOVERY

SIPSE-CSIRT, continuità e ripristino

06

INDEPENDENT ASSURANCE

Audit, verifiche e certificazione indipendente

Allegato tecnico B – Matrice delle responsabilità

Funzione	Responsabile	Controllo
Identità	Unità anagrafica	Audit
Abilitazione	Ufficio consultazioni	Verifica indipendente
Voto	Unità elettorale digitale	Audit crittografico
Scrutinio	Unità di scrutinio	Controllo distribuito
Sicurezza	SIPSE-SOC	Comitato sicurezza
Incidenti	SIPSE-CSIRT	Audit successivo
Ripristino	Direzione tecnica	Verifica integrità
Certificazione	Organismo indipendente	DPS-04

Allegato tecnico C – Indicatori di sicurezza

Propongo l'istituzione di un sistema permanente di indicatori, denominato SIPSE-Security Index.

Indicatore	Misurazione
Disponibilità	Percentuale di operatività
Integrità	Anomalie nelle registrazioni
Sicurezza	Vulnerabilità aperte
Continuità	Tempi effettivi di ripristino
Autenticazione	Accessi anomali
Incidenti	Numero e gravità
Audit	Non conformità rilevate
Resilienza	Esito delle simulazioni

Gli indicatori devono essere pubblicati in forma aggregata, senza divulgare informazioni che possano facilitare attacchi.

Allegato tecnico D – Una garanzia ulteriore: il principio dei tre controlli indipendenti

Ritengo particolarmente importante introdurre un meccanismo che distingua tre responsabilità:

Primo controllo

Integrità tecnologica

Il sistema ha funzionato secondo le configurazioni autorizzate?

Secondo controllo

Integrità democratica

La partecipazione e lo scrutinio hanno rispettato le garanzie previste?

Terzo controllo

Integrità documentale

Il risultato pubblicato corrisponde agli atti e alle verifiche conservate?

La certificazione finale dovrebbe essere rilasciata soltanto dopo l'esame delle tre dimensioni. Una certificazione tecnica non deve essere confusa con una certificazione della legittimità giuridica della consultazione.

Riferimenti tecnici internazionali

La struttura proposta si coordina con documenti e orientamenti tecnici già esistenti:

1. NIST Cybersecurity Framework 2.0: organizza la gestione del rischio nelle sei funzioni Govern, Identify, Protect, Detect, Respond e Recover.

   NIST

2. NIST Election Infrastructure Profile: riferimento specifico per la protezione delle infrastrutture informatiche elettorali.

   NIST

3. ENISA: orientamenti sulla protezione dei processi elettorali dalle minacce informatiche e ibride.

   Shaping Europe’s digital future

4. NIST Election Security Guides: autenticazione multifattore, comunicazioni affidabili e integrità dei dati.

NIST