S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

CANCELLERIA GENERALE
SEGRETERIA TECNICA PER L'EFFETTIVITÀ E LA CONFORMITÀ DEI DIRITTI

ATTO N. 03/CCJC

MANUALE GENERALE DI AUDIT, VERIFICA E VALUTAZIONE DELLA CONFORMITÀ

Codice: SIPSE-CCJC-MAN-03/2026
Versione: 1.0
Data di emissione: 13 novembre 2026
Stato: Documento predisposto per approvazione
Applicazione: Sistema volontario di certificazione SIPSE-CCJC

PREMESSA

Il presente Manuale disciplina le procedure tecniche, documentali, organizzative e decisionali attraverso le quali il sistema SIPSE-CCJC realizza la valutazione della conformità dei soggetti richiedenti rispetto ai requisiti stabiliti dal Disciplinare Generale e dai relativi schemi di certificazione.

Il Manuale costituisce lo strumento operativo di riferimento per:

- la Segreteria Tecnica;
- gli auditor e i valutatori;
- il Comitato Indipendente di Valutazione e Certificazione;
- il Collegio di Garanzia e Riesame, per le materie di propria competenza;
- l'Unità Tecnologica e di Integrità Documentale;
- i soggetti richiedenti la certificazione.

Il sistema adotta una metodologia basata su evidenze verificabili, criteri preventivamente dichiarati, proporzionalità delle verifiche, gestione del rischio, tracciabilità delle attività e indipendenza delle decisioni.

La certificazione SIPSE-CCJC è un'attestazione volontaria di conformità rispetto a un perimetro e a requisiti esplicitamente individuati. Non costituisce immunità, autorizzazione pubblica, accreditamento, riconoscimento statale o attestazione universale di conformità all'intero ordinamento giuridico internazionale.

PARTE I – PRINCIPI E DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente Manuale disciplina l'intero processo di audit, verifica e valutazione della conformità ai fini del rilascio, mantenimento, estensione, rinnovo, sospensione e revoca della certificazione SIPSE-CCJC.
2. Sono disciplinate le seguenti fasi:

   a. presentazione della domanda;

   b. analisi preliminare;

   c. definizione del perimetro;

   d. pianificazione dell'audit;

   e. verifica documentale;

   f. verifica tecnica e organizzativa;

   g. raccolta delle evidenze;

   h. classificazione delle risultanze;

   i. valutazione delle non conformità;

   j. predisposizione del rapporto conclusivo;

   k. decisione indipendente;

   l. sorveglianza successiva.

Articolo 2 – Finalità

Il Manuale persegue le seguenti finalità:

1. assicurare uniformità metodologica tra le verifiche;
2. ridurre la discrezionalità non motivata;
3. garantire verificabilità e ripetibilità delle valutazioni;
4. assicurare la tracciabilità delle evidenze;
5. tutelare i diritti degli interessati;
6. individuare e prevenire rischi organizzativi, giuridici e tecnologici;
7. rendere verificabile il processo di certificazione;
8. garantire l'indipendenza del giudizio tecnico;

9. consentire la comparabilità delle valutazioni;
10. favorire il miglioramento continuo dei soggetti certificati.

Articolo 3 – Riferimenti metodologici

1. Il sistema utilizza, ove pertinenti e compatibili con il proprio campo di applicazione, i principi contenuti in:

   a. ISO/IEC 17000 – Vocabolario e principi generali della valutazione della conformità;

   b. ISO/IEC 17065 – Requisiti per gli organismi che certificano prodotti, processi e servizi;

   c. ISO/IEC 17020 – Criteri generali per il funzionamento dei vari tipi di organismi che effettuano attività di ispezione;

   d. ISO/IEC 27001 – Sistemi di gestione della sicurezza delle informazioni;

   e. ISO/IEC 27701 – Gestione delle informazioni sulla privacy;

   f. ISO/IEC 42001 – Sistemi di gestione dell'intelligenza artificiale;

   g. ISO 19011 – Linee guida per gli audit dei sistemi di gestione;

   h. ISO/IEC 27005 – Gestione dei rischi per la sicurezza delle informazioni.

2. Sono inoltre considerati, secondo il campo di applicazione e la normativa pertinente:

   a. Dichiarazione universale dei diritti umani;

   b. Patto internazionale sui diritti civili e politici;

   c. Patto internazionale sui diritti economici, sociali e culturali;

   d. Convenzione europea dei diritti dell'uomo;

   e. Regolamento (UE) 2016/679;

   f. Regolamento (UE) 2022/2065 sui servizi digitali;

   g. Regolamento (UE) 2024/1689 sull'intelligenza artificiale;

   h. normativa nazionale applicabile;

   i. convenzioni internazionali pertinenti e vincolanti per i soggetti interessati.

3. Il richiamo a uno standard non implica automaticamente conformità, certificazione, accreditamento o autorizzazione all'uso dei relativi marchi.
4. La Segreteria Tecnica mantiene un repertorio aggiornato dei riferimenti normativi e tecnici applicabili.

Articolo 4 – Principi di valutazione

Ogni audit è condotto secondo i principi di:

a. integrità;

b. imparzialità;

c. competenza;

d. riservatezza;

e. indipendenza;

f. approccio basato sulle evidenze;

g. approccio basato sul rischio;

h. proporzionalità;

i. trasparenza metodologica;

j. responsabilità documentale;

k. riproducibilità delle verifiche.

Articolo 5 – Oggetto della certificazione

1. La certificazione può riguardare:

   a. un'impresa;

   b. un'organizzazione;

   c. un servizio digitale;

   d. una piattaforma telematica;

   e. un'infrastruttura tecnologica;

   f. un sistema di gestione;

   g. un processo organizzativo;

   h. un sistema algoritmico;

   i. un servizio di trattamento o gestione dei dati;

   j. un sistema di integrità e conservazione documentale.

2. Il certificato deve indicare con precisione il soggetto, il servizio, il processo, l'infrastruttura o il sistema effettivamente valutato.
3. Non è consentito estendere implicitamente la certificazione a prodotti, servizi, società controllate o infrastrutture non comprese nel perimetro sottoposto ad audit.

PARTE II – SCHEMI DI CERTIFICAZIONE

Articolo 6 – Articolazione degli schemi

Il sistema SIPSE-CCJC prevede cinque schemi principali:

1. CCJC-DIG – Conformità giuridica e digitale

Valuta la governance giuridica del servizio, la chiarezza delle condizioni contrattuali, il rispetto dei diritti degli utenti e la gestione degli obblighi applicabili.

2. CCJC-DAT – Protezione e governance dei dati

Valuta la gestione dei dati personali e non personali, la trasparenza dei trattamenti, la sicurezza, i diritti degli interessati e la responsabilità organizzativa.

3. CCJC-INF – Integrità delle infrastrutture

Valuta la sicurezza, la continuità operativa, la resilienza, il controllo degli accessi, la gestione delle vulnerabilità e la protezione delle infrastrutture.

4. CCJC-ALG – Trasparenza e responsabilità algoritmica

Valuta la documentazione dei sistemi algoritmici, la gestione dei rischi, la supervisione umana, la trasparenza e le procedure di contestazione.

5. CCJC-IMP – Integrità documentale e probatoria

Valuta i processi di formazione, autenticazione, conservazione, registrazione, verifica e tracciabilità dei documenti e delle evidenze digitali.

Articolo 7 – Certificazione singola e integrata

1. Il richiedente può presentare domanda per uno o più schemi.
2. È possibile rilasciare una certificazione integrata quando più schemi siano stati effettivamente verificati.
3. Ogni schema mantiene la propria identificazione e i propri risultati.
4. La certificazione integrata non può essere utilizzata per far presumere la verifica di requisiti non inclusi nell'audit.

Articolo 8 – Livelli di verifica

Il sistema prevede tre livelli:

Livello A – Verifica documentale

Esame della documentazione, delle politiche, delle procedure e delle evidenze messe a disposizione dal richiedente.

Livello B – Verifica documentale e operativa

Comprende il Livello A e l'esame delle modalità effettive di funzionamento dei processi, mediante interviste, campionamenti e verifiche tecniche.

Livello C – Verifica approfondita

Comprende i livelli precedenti e, quando legittimo, proporzionato e tecnicamente possibile, test tecnici, analisi di configurazione, prove di sicurezza, verifiche sul campo e valutazioni specialistiche.

Il livello applicato deve essere dichiarato nel piano di audit e nel certificato.

PARTE III – PROCEDURA DI ACCESSO E PIANIFICAZIONE

Articolo 9 – Presentazione della domanda

1. La domanda è presentata mediante il Modulo CCJC-01.
2. Il richiedente identifica:

   a. soggetto giuridico o organizzativo;

   b. rappresentante o referente autorizzato;

   c. servizio o infrastruttura;

   d. schema o schemi richiesti;

   e. sedi e infrastrutture interessate;

   f. eventuali fornitori essenziali;

   g. principali trattamenti di dati;

   h. sistemi tecnologici coinvolti;

   i. documentazione disponibile.

3. Il richiedente dichiara la correttezza delle informazioni trasmesse e l'autorizzazione alla verifica delle evidenze comprese nel perimetro.
4. La domanda non comporta diritto automatico al rilascio della certificazione.

Articolo 10 – Analisi preliminare

1. La Segreteria Tecnica verifica la completezza amministrativa e tecnica della domanda.
2. La verifica preliminare accerta:

   a. identificabilità del richiedente;

   b. identificabilità dell'oggetto;

   c. definizione del perimetro;

   d. disponibilità minima della documentazione;

   e. competenza tecnica necessaria;

   f. assenza di impedimenti procedurali evidenti.

3. Se la documentazione è incompleta, sono richieste integrazioni.
4. La Segreteria può dichiarare la domanda non procedibile, con motivazione, quando l'oggetto non sia identificabile o non rientri negli schemi applicabili.

Articolo 11 – Definizione del perimetro

1. Il perimetro determina l'estensione effettiva della valutazione.
2. Deve indicare:

   a. soggetto richiedente;

   b. servizio o sistema;

   c. processi inclusi;

   d. sedi e infrastrutture interessate;

   e. sistemi esternalizzati rilevanti;

   f. categorie di dati coinvolti;

   g. utenti o destinatari interessati;

   h. eventuali esclusioni motivate.

3. Ogni esclusione deve essere documentata e non può compromettere la validità delle conclusioni.
4. Il perimetro è approvato dal richiedente e registrato nel fascicolo.

Articolo 12 – Analisi del rischio preliminare

1. La Segreteria Tecnica effettua una valutazione preliminare del rischio.
2. Sono considerati:

   a. natura del servizio;

   b. numero e tipologia degli utenti;

   c. criticità dei dati;

   d. dipendenza da infrastrutture esterne;

   e. impatto di eventuali incidenti;

   f. utilizzo di sistemi automatizzati;

   g. impatto potenziale sui diritti fondamentali;

   h. complessità tecnologica;

   i. esposizione a minacce informatiche;

   j. capacità organizzativa del richiedente.

3. La valutazione determina l'intensità e l'estensione dell'audit.

Articolo 13 – Piano di audit

1. La Segreteria Tecnica redige un piano di audit.
2. Il piano indica:

   a. obiettivi;

   b. criteri;

   c. perimetro;

   d. livello di verifica;

   e. durata;

   f. auditor assegnati;

   g. modalità di accesso alle evidenze;

   h. verifiche previste;

   i. eventuali test;

j. calendario;

k. modalità di comunicazione dei risultati.

3. Il richiedente riceve il piano prima dell'avvio delle verifiche.
4. Le modifiche sostanziali sono motivate e registrate.

PARTE IV – ATTIVITÀ DI AUDIT

Articolo 14 – Riunione di apertura

L'audit inizia con una riunione di apertura nella quale sono:

a. identificati i partecipanti;

b. confermati gli obiettivi;

c. confermato il perimetro;

d. illustrate le modalità di verifica;

e. concordate le modalità operative;

f. richiamati gli obblighi di riservatezza;

g. definiti i referenti del richiedente.

Articolo 15 – Verifica documentale

1. La verifica documentale esamina, in relazione allo schema richiesto:

   a. atti costitutivi e documenti identificativi;

   b. organigrammi;

   c. politiche e procedure;

   d. contratti e condizioni di servizio;

   e. informative agli utenti;

   f. registri dei trattamenti, ove applicabili;

   g. valutazioni d'impatto, ove necessarie;

   h. registri degli incidenti;

i. piani di continuità;

j. politiche di sicurezza;

k. documentazione algoritmica;

l. procedure di reclamo;

m. registri di conservazione documentale;

n. evidenze di formazione del personale.

2. L'auditor registra la documentazione esaminata, la versione, la data e la provenienza.
3. La sola esistenza formale di una procedura non prova la sua effettiva applicazione.

Articolo 16 – Verifica operativa

La verifica operativa può comprendere:

a. interviste al personale;

b. osservazione dei processi;

c. esame di registri e log;

d. verifica di campioni documentali;

e. controllo degli accessi;

f. analisi dei processi di gestione dei dati;

g. verifica delle procedure di reclamo;

h. simulazione di scenari di incidente;

i. esame dei processi di aggiornamento e manutenzione;

j. verifica delle misure correttive.

Le attività sono limitate al perimetro autorizzato e devono rispettare la normativa applicabile.

Articolo 17 – Verifiche tecniche e test

1. I test tecnici sono svolti esclusivamente in presenza di autorizzazione adeguata e di condizioni di sicurezza.
2. Possono comprendere:

   a. verifica delle configurazioni;

   b. analisi delle vulnerabilità;

c. test di sicurezza autorizzati;

d. verifica della cifratura;

e. controllo delle procedure di backup;

f. verifica della gestione delle credenziali;

g. test di ripristino;

h. verifica dei meccanismi di autenticazione;

i. analisi dei registri di sistema;

j. test di integrità documentale.

3. Sono vietati test intrusivi non autorizzati, accessi abusivi, esfiltrazione di dati e attività che possano compromettere la continuità del servizio.
4. Ogni test è documentato indicando ambiente, autorizzazione, strumenti, limiti, risultati e anomalie.

Articolo 18 – Campionamento

1. Quando non sia ragionevole o necessario verificare l'intera popolazione documentale o tecnica, l'auditor può utilizzare un campionamento.
2. Il campionamento deve essere motivato e proporzionato.
3. Il rapporto indica:

   a. popolazione di riferimento;

   b. dimensione del campione;

   c. criterio di selezione;

   d. periodo considerato;

   e. eventuali limiti statistici.

4. Il campionamento non può essere presentato come verifica integrale.

Articolo 19 – Evidenze di audit

1. Ogni risultanza deve essere sostenuta da evidenze sufficienti, pertinenti e verificabili.
2. Le evidenze possono consistere in:

   a. documenti;

   b. registrazioni;

   c. log;

d. dichiarazioni corroborate;

e. osservazioni dirette;

f. risultati di test;

g. configurazioni;

h. registri elettronici;

i. firme e marcature temporali;

j. impronte crittografiche.

3. Le dichiarazioni del richiedente, se non corroborate, sono identificate come dichiarazioni e non come prove indipendenti.
4. L'auditor deve distinguere fatti osservati, informazioni dichiarate, inferenze tecniche e valutazioni professionali.

Articolo 20 – Integrità delle evidenze

1. Le evidenze digitali rilevanti sono identificate con un codice univoco.
2. Quando opportuno, sono registrati:

   a. nome del documento;

   b. formato;

   c. data di acquisizione;

   d. soggetto che lo ha fornito;

   e. modalità di acquisizione;

   f. impronta crittografica;

   g. eventuale firma elettronica;

   h. eventuale marcatura temporale;

   i. collocazione nel fascicolo.

3. L'utilizzo di SHA-256 o di altri strumenti crittografici è finalizzato a verificare l'integrità dei file rispetto all'impronta registrata.
4. La registrazione dell'impronta non certifica la veridicità sostanziale del contenuto.
5. La catena di custodia documentale deve consentire di ricostruire i passaggi essenziali dell'acquisizione e della conservazione.

PARTE V – CRITERI DI CONFORMITÀ

Articolo 21 – Struttura dei requisiti

1. I requisiti sono classificati in:

   a. requisiti obbligatori;

   b. requisiti tecnici;

   c. requisiti organizzativi;

   d. requisiti di miglioramento;

   e. requisiti specifici dello schema.

2. Ogni requisito deve essere associato a:

   a. codice;

   b. descrizione;

   c. criterio di valutazione;

   d. evidenza richiesta;

   e. metodo di verifica;

   f. livello di criticità.

3. Il catalogo dei requisiti è mantenuto dalla Segreteria Tecnica e approvato dall'organo competente.

Articolo 22 – Requisiti generali

Sono oggetto di verifica, secondo il perimetro:

1. identificabilità e responsabilità del soggetto;
2. trasparenza organizzativa;
3. chiarezza dei rapporti contrattuali;
4. rispetto dei diritti degli utenti;
5. sicurezza dei dati e delle infrastrutture;
6. gestione delle vulnerabilità;
7. gestione degli incidenti;
8. continuità operativa;
9. gestione dei fornitori;
10. tracciabilità delle attività;
11. gestione dei reclami;
12. supervisione dei processi automatizzati;

13. controllo degli accessi;
14. correttezza delle informazioni pubblicate;
15. disponibilità di procedure di correzione.

Articolo 23 – Diritti fondamentali

1. La valutazione considera, nei limiti del perimetro e della normativa applicabile:

   a. dignità della persona;

   b. non discriminazione;

   c. tutela della riservatezza;

   d. protezione dei dati personali;

   e. libertà di espressione e informazione;

   f. accessibilità;

   g. trasparenza;

   h. possibilità di contestazione;

   i. tutela contro decisioni automatizzate illegittime;

   j. accesso ai rimedi previsti dall'ordinamento applicabile.

2. L'audit verifica l'esistenza e l'effettività delle misure organizzative e tecniche pertinenti.
3. Il sistema non sostituisce l'autorità giudiziaria nella determinazione definitiva di responsabilità giuridiche.

Articolo 24 – Requisiti di sicurezza digitale

Sono valutati, secondo il rischio:

a. gestione delle identità;

b. autenticazione;

c. autorizzazione;

d. segregazione dei privilegi;

e. cifratura;

f. aggiornamento dei sistemi;

g. gestione delle vulnerabilità;

h. registrazione degli eventi;

i. backup;

j. ripristino;

k. gestione degli incidenti;

l. sicurezza della catena di fornitura.

Articolo 25 – Requisiti per i sistemi algoritmici

Quando il perimetro comprende sistemi algoritmici o di intelligenza artificiale, sono valutati, ove pertinenti:

a. finalità dichiarata;

b. documentazione del sistema;

c. provenienza e qualità dei dati;

d. analisi dei rischi;

e. possibili effetti discriminatori;

f. supervisione umana;

g. tracciabilità delle decisioni;

h. procedure di contestazione;

i. monitoraggio successivo;

j. gestione delle modifiche;

k. sicurezza e robustezza;

l. obblighi normativi specificamente applicabili.

Articolo 26 – Requisiti di integrità documentale

Sono valutati:

a. identificazione dei documenti;

b. controllo delle versioni;

c. autenticazione delle operazioni;

d. integrità dei file;

e. tracciabilità delle modifiche;

f. conservazione;

g. disponibilità;

h. controllo degli accessi;

i. procedure di verifica;

j. gestione delle copie e dei duplicati.

PARTE VI – CLASSIFICAZIONE DELLE RISULTANZE

Articolo 27 – Classificazione generale

Le risultanze dell'audit sono classificate in:

A. Conformità

Il requisito è soddisfatto sulla base delle evidenze raccolte.

B. Osservazione

È rilevata una circostanza che non costituisce non conformità, ma può comportare un rischio o un possibile peggioramento.

C. Non conformità minore

È rilevata una deviazione circoscritta che non compromette in modo sostanziale il requisito o il funzionamento complessivo del sistema valutato.

D. Non conformità maggiore

È rilevata una violazione significativa di un requisito obbligatorio, una carenza sistemica o un'assenza di controllo capace di compromettere l'affidabilità del servizio rispetto al perimetro certificato.

E. Criticità grave

È rilevata una situazione che presenta un rischio grave o immediato per diritti, sicurezza, integrità o continuità del servizio, oppure evidenze di condotte fraudolente o di falsificazione documentale.

Articolo 28 – Criteri di classificazione

1. La classificazione considera:

   a. gravità;

   b. probabilità;

   c. impatto;

   d. estensione;

   e. durata;

   f. ripetitività;

   g. vulnerabilità degli interessati;

   h. efficacia dei controlli esistenti;

   i. capacità di rilevazione e correzione.

2. La classificazione deve essere motivata e documentata.
3. La gravità non può essere ridotta esclusivamente in ragione dell'assenza di reclami o incidenti segnalati.

Articolo 29 – Gestione delle non conformità

1. Ogni non conformità deve essere descritta indicando:

   a. requisito violato;

   b. evidenza oggettiva;

   c. circostanza rilevata;

   d. rischio associato;

   e. classificazione;

   f. correzione richiesta;

   g. termine per il riscontro.

2. Il richiedente può presentare osservazioni e contestazioni tecniche.
3. L'auditor valuta le osservazioni e motiva l'eventuale conferma o modifica della classificazione.
4. Il Comitato decide sulla base del fascicolo completo.

Articolo 30 – Azioni correttive

1. Il richiedente deve predisporre un piano di azioni correttive per le non conformità rilevate.

2. Il piano indica:

   a. causa individuata;

   b. correzione immediata;

   c. azione correttiva;

   d. responsabile;

   e. termine;

   f. modalità di verifica dell'efficacia.

3. La mera dichiarazione di aver corretto una carenza non equivale alla dimostrazione dell'efficacia della correzione.
4. Le non conformità maggiori devono essere chiuse prima del rilascio della certificazione.
5. Le non conformità minori possono essere gestite mediante piano di correzione con termine definito, purché non compromettano i requisiti essenziali dello schema.
6. Le criticità gravi impediscono il rilascio fino alla loro risoluzione e alla verifica indipendente delle misure adottate.

PARTE VII – RAPPORTO DI AUDIT E DECISIONE

Articolo 31 – Riunione di chiusura

Al termine delle verifiche l'auditor:

a. presenta le risultanze preliminari;

b. illustra le non conformità;

c. consente al richiedente di formulare osservazioni;

d. chiarisce eventuali limiti dell'audit;

e. indica le fasi successive;

f. registra eventuali dissensi.

La riunione di chiusura non costituisce decisione di certificazione.

Articolo 32 – Rapporto di audit

1. Il rapporto di audit contiene almeno:

a. codice della pratica;

b. soggetto valutato;

c. perimetro;

d. schema applicato;

e. livello di verifica;

f. auditor;

g. date delle verifiche;

h. documentazione esaminata;

i. attività svolte;

j. evidenze raccolte;

k. risultanze;

l. non conformità;

m. eventuali limitazioni;

n. conclusioni tecniche.

2. Il rapporto deve distinguere le evidenze oggettive dalle opinioni professionali.
3. Il rapporto è sottoscritto dai valutatori responsabili.

Articolo 33 – Revisione tecnica interna

1. Prima della trasmissione al Comitato, la Segreteria Tecnica verifica la completezza formale del rapporto.
2. La revisione controlla:

   a. coerenza tra perimetro e verifiche;

   b. completezza delle evidenze;

   c. corretta classificazione;

   d. tracciabilità delle risultanze;

   e. adeguatezza delle conclusioni.

3. La revisione non può modificare arbitrariamente le conclusioni dell'auditor.
4. Ogni richiesta di integrazione deve essere registrata.

Articolo 34 – Decisione indipendente

1. Il Comitato Indipendente esamina il fascicolo conclusivo.
2. La decisione può consistere in:

   a. rilascio della certificazione;

   b. rilascio con limitazioni espressamente indicate;

   c. richiesta di integrazioni;

   d. sospensione della decisione in attesa di ulteriori verifiche;

   e. diniego motivato.

3. Il Comitato può richiedere una nuova valutazione quando le evidenze siano insufficienti o contraddittorie.
4. La decisione è autonoma rispetto all'attività dell'auditor e della Segreteria Tecnica.

Articolo 35 – Motivazione della decisione

La decisione deve indicare:

a. oggetto;

b. perimetro;

c. schema;

d. criteri applicati;

e. documentazione esaminata;

f. esito delle verifiche;

g. non conformità rilevanti;

h. eventuali limitazioni;

i. durata;

j. condizioni di mantenimento;

k. modalità di riesame.

Articolo 36 – Emissione del certificato

1. Dopo la decisione favorevole, la Cancelleria procede all'emissione amministrativa del certificato.

2. Il certificato contiene:

   a. logo e identificazione SIPSE-CCJC;

   b. codice univoco;

   c. soggetto certificato;

   d. oggetto e perimetro;

   e. schema o schemi;

   f. livello di verifica;

   g. data di rilascio;

   h. data di scadenza;

   i. riferimento alla decisione;

   j. identificativo di verifica pubblica.

3. Il certificato è firmato dal soggetto autorizzato secondo le procedure interne.
4. Il certificato non può contenere dichiarazioni di immunità o di prevalenza automatica sulle leggi applicabili.

PARTE VIII – DURATA, SORVEGLIANZA E RINNOVO

Articolo 37 – Durata

1. La certificazione ha durata ordinaria di dodici mesi, salvo diversa durata motivata prevista dallo specifico schema.
2. La durata decorre dalla data di emissione.
3. Il certificato indica espressamente la propria scadenza.
4. Il rinnovo non è automatico.

Articolo 38 – Sorveglianza

1. La Segreteria Tecnica programma verifiche di sorveglianza durante il periodo di validità.
2. La sorveglianza può comprendere:

   a. aggiornamenti documentali;

   b. verifiche a campione;

c. esame degli incidenti;

d. verifica delle azioni correttive;

e. controllo delle modifiche sostanziali;

f. verifica della permanenza dei requisiti.

3. La frequenza è definita in base al rischio e allo schema applicato.

Articolo 39 – Obbligo di comunicazione delle modifiche

Il soggetto certificato comunica tempestivamente:

a. modifiche societarie rilevanti;

b. cambiamenti del perimetro;

c. modifiche infrastrutturali sostanziali;

d. cambiamenti significativi nei sistemi algoritmici;

e. incidenti rilevanti;

f. violazioni significative;

g. sospensioni o revoche di autorizzazioni pubbliche pertinenti;

h. cambiamenti che possano incidere sui requisiti certificati.

Articolo 40 – Rinnovo

1. Il rinnovo richiede una nuova verifica della permanenza dei requisiti.
2. La verifica considera:

   a. risultati della sorveglianza;

   b. incidenti;

   c. modifiche intervenute;

   d. reclami;

   e. azioni correttive;

   f. aggiornamenti normativi;

   g. evoluzione del rischio.

3. Il Comitato decide autonomamente sul rinnovo.

Articolo 41 – Sospensione

La certificazione può essere sospesa quando:

a. siano emerse non conformità rilevanti;

b. il soggetto non consenta le verifiche previste;

c. siano fornite informazioni materialmente inesatte;

d. non siano attuate le azioni correttive;

e. sia compromessa l'affidabilità delle evidenze;

f. siano intervenute modifiche non comunicate che incidano sul perimetro.

La sospensione è motivata, comunicata e registrata.

Articolo 42 – Revoca

La revoca può essere disposta in caso di:

a. frode documentale;

b. falsificazione di evidenze;

c. violazione grave e non rimediata dei requisiti;

d. reiterata inosservanza del Disciplinare;

e. perdita definitiva dei requisiti essenziali;

f. uso ingannevole della certificazione;

g. impossibilità di verificare l'oggetto certificato.

La revoca è deliberata dal Comitato secondo la procedura applicabile.

PARTE IX – RECLAMI, RICORSI E GARANZIE

Articolo 43 – Reclami

1. Il soggetto certificato, il richiedente o altro soggetto legittimamente interessato può presentare reclamo secondo il regolamento applicabile.

2. Il reclamo deve identificare:

   a. reclamante;

   b. oggetto;

   c. fatti;

   d. documentazione disponibile;

   e. richiesta formulata.

3. Il reclamo è protocollato dalla Cancelleria e trasmesso all'organo competente.

Articolo 44 – Riesame

1. Le decisioni del Comitato sono impugnabili mediante riesame interno secondo il regolamento del Collegio di Garanzia.
2. Il riesame riguarda la regolarità procedurale, l'imparzialità, la corretta applicazione dei criteri e l'adeguatezza della motivazione.
3. Il Collegio non può sostituire il proprio giudizio tecnico a quello del Comitato senza adeguata base procedurale e motivazione.
4. Restano impregiudicati i rimedi previsti dalla normativa applicabile.

Articolo 45 – Protezione del richiedente e contraddittorio

1. Il richiedente deve essere informato delle risultanze che possono determinare il diniego, la sospensione o la revoca.
2. Deve essere garantita la possibilità di presentare osservazioni entro un termine congruo.
3. Nei casi di rischio grave e immediato, possono essere adottate misure cautelative interne, proporzionate e motivate, con successiva possibilità di contestazione.

PARTE X – RISERVATEZZA, DATI E SICUREZZA

Articolo 46 – Riservatezza

1. Tutte le informazioni acquisite durante l'audit sono trattate come riservate, salvo quelle destinate legittimamente alla pubblicazione.
2. L'accesso è limitato ai soggetti autorizzati.
3. La diffusione a terzi richiede una base giuridica o un'autorizzazione valida.

Articolo 47 – Protezione dei dati personali

1. Il trattamento dei dati personali avviene nel rispetto della normativa applicabile.

2. Devono essere definiti, secondo i ruoli effettivi, titolare, eventuali responsabili e soggetti autorizzati al trattamento.
3. Devono essere applicati principi di minimizzazione, limitazione delle finalità, sicurezza e conservazione limitata.
4. Il sistema non acquisisce dati personali eccedenti rispetto alle finalità della certificazione.

Articolo 48 – Sicurezza del fascicolo

Il fascicolo di audit deve essere protetto mediante:

a. autenticazione degli utenti;

b. controllo degli accessi;

c. registrazione delle operazioni;

d. protezione delle copie;

e. backup;

f. procedure di ripristino;

g. cifratura ove appropriata;

h. gestione delle autorizzazioni;

i. conservazione documentale controllata.

PARTE XI – INDICATORI, QUALITÀ E MIGLIORAMENTO

Articolo 49 – Indicatori di qualità

Il sistema utilizza almeno i seguenti indicatori:

1. tempo medio di gestione delle domande;
2. percentuale di pratiche complete al primo invio;
3. numero di audit conclusi;
4. numero di non conformità rilevate;
5. percentuale di azioni correttive chiuse;
6. numero di reclami ricevuti;
7. tempo medio di risoluzione dei reclami;
8. numero di certificazioni sospese o revocate;
9. numero di incidenti documentali;
10. percentuale di verifiche di sorveglianza eseguite.

Articolo 50 – Riesame periodico del Manuale

1. Il Manuale è riesaminato almeno annualmente.
2. Il riesame considera:

   a. evoluzione normativa;

   b. aggiornamenti tecnici;

   c. risultati degli audit;

   d. reclami;

   e. criticità organizzative;

   f. incidenti;

   g. proposte di miglioramento.

3. Le modifiche sono approvate dall'organo competente.
4. Ogni versione deve riportare numero, data, descrizione delle modifiche e soggetto approvante.

Articolo 51 – Formazione degli auditor

1. Gli auditor devono possedere competenze adeguate allo schema di certificazione.
2. La Segreteria Tecnica mantiene un registro delle qualificazioni.
3. La formazione comprende:

   a. principi di audit;

   b. criteri di conformità;

   c. diritti fondamentali;

   d. protezione dei dati;

   e. sicurezza digitale;

   f. gestione delle evidenze;

   g. conflitti d'interesse;

   h. redazione dei rapporti.

4. Il sistema può prevedere aggiornamenti periodici e verifiche della competenza.

Articolo 52 – Valutazione dell'attività degli auditor

La Segreteria Tecnica valuta periodicamente:

a. qualità dei rapporti;

b. coerenza delle classificazioni;

c. capacità di raccolta delle evidenze;

d. rispetto dei tempi;

e. imparzialità;

f. gestione dei rapporti con i richiedenti;

g. rispetto delle procedure.

In caso di carenze può disporre formazione, affiancamento, limitazione delle competenze o sospensione dall'elenco degli auditor.

PARTE XII – DISPOSIZIONI FINALI

Articolo 53 – Gerarchia documentale

Il presente Manuale è subordinato:

1. agli atti costitutivi e alle regole interne del SIPSE;
2. alla Deliberazione istitutiva n. 01/CCJC;
3. al Disciplinare Generale SIPSE-CCJC-REG-01;
4. al Decreto n. 02/CCJC;
5. ai regolamenti specifici approvati dagli organi competenti.

In caso di contrasto prevalgono le disposizioni di livello superiore, ferma restando la normativa applicabile.

Articolo 54 – Interpretazione

1. Le disposizioni sono interpretate in modo da assicurare imparzialità, verificabilità e coerenza con lo scopo della certificazione.
2. I dubbi tecnici sono sottoposti alla Segreteria Tecnica.
3. Le questioni relative alla decisione di certificazione spettano al Comitato.
4. Le questioni relative ai reclami e ai ricorsi spettano al Collegio di Garanzia.

Articolo 55 – Entrata in vigore

1. Il Manuale entra in vigore dopo l'approvazione dell'organo competente.
2. È applicabile alle domande presentate successivamente alla sua entrata in vigore.

3. Le pratiche già avviate possono essere adeguate alle nuove disposizioni, previa comunicazione ai richiedenti e senza pregiudicare i diritti già maturati.

ALLEGATO 1

MATRICE GENERALE DEI REQUISITI CCJC

Codice	Area	Requisito	Evidenza principale
GOV-01	Governance	Responsabilità organizzative definite	Organigramma e deleghe
GOV-02	Governance	Politiche documentate	Politiche approvate
LEG-01	Giuridica	Obblighi applicabili identificati	Registro normativo
LEG-02	Giuridica	Condizioni di servizio trasparenti	Contratti e informative
DIR-01	Diritti	Procedure per i diritti degli utenti	Procedure e registri
DAT-01	Dati	Gestione dei dati documentata	Registro e procedure
DAT-02	Dati	Controllo degli accessi	Log e configurazioni
INF-01	Infrastruttura	Gestione delle vulnerabilità	Registro e rapporti
INF-02	Infrastruttura	Continuità operativa	Piano di continuità
INF-03	Infrastruttura	Gestione degli incidenti	Registro incidenti
ALG-01	Algoritmi	Documentazione dei sistemi	Scheda tecnica
ALG-02	Algoritmi	Supervisione e controllo	Procedure e registri
IMP-01	Integrità	Identificazione documentale	Registro documenti
IMP-02	Integrità	Verifica dell'integrità	Hash e registri
IMP-03	Integrità	Conservazione e tracciabilità	Log e procedure

La matrice è una base generale. I requisiti specifici devono essere dettagliati negli schemi tecnici approvati.

ALLEGATO 2

MODELLO DI RAPPORTO DI AUDIT

Codice pratica: _____
Richiedente: _____
Oggetto: _____
Schema: _____
Perimetro: _____
Livello di verifica: _____
Auditor: _____
Data: _____

1. Obiettivi dell'audit

---

2. Criteri applicati

---

3. Documentazione esaminata

---

4. Verifiche effettuate

---

5. Evidenze raccolte

---

6. Risultanze

Codice requisito Esito Evidenza Osservazioni

7. Non conformità

---

8. Limitazioni dell'audit

---

9. Conclusioni tecniche

Firma auditor: _____

Data: _____

ALLEGATO 3

MODELLO DI SCHEDA DI NON CONFORMITÀ

Codice NC: _____
Codice pratica: _____
Requisito: _____
Classificazione: _____

Descrizione della circostanza rilevata:

Evidenza oggettiva:

Rischio associato:

Azione immediata richiesta:

Azione correttiva proposta:

Responsabile dell'attuazione:

Termine:

Verifica dell'efficacia:

Esito della verifica:

[ ] Chiusa
[ ] Non chiusa
[ ] Necessario approfondimento

Firma del valutatore: _____

ALLEGATO 4

MODELLO DI DELIBERA DI CERTIFICAZIONE

Comitato Indipendente di Valutazione e Certificazione SIPSE-CCJC

Codice pratica: _____

Richiedente: _____

Oggetto: _____

Schema: _____

Esaminati il rapporto di audit, le evidenze e la documentazione del fascicolo;

verificata la completezza dell'istruttoria;

valutata la conformità ai requisiti applicabili;

IL COMITATO DELIBERA

[ ] Rilascio della certificazione

[ ] Rilascio con limitazioni

[ ] Richiesta di integrazioni

[ ] Sospensione della decisione

[ ] Diniego motivato

Motivazione:

Perimetro certificato:

Durata:

Condizioni di mantenimento:

Presidente: _____

Componenti: _____

Data: _____

ALLEGATO 5

MODELLO DI REGISTRO DELLE EVIDENZE DIGITALI

ID Documento Data acquisizione Provenienza Hash Responsabile

EVD-001
EVD-002
EVD-003

Il registro deve consentire di ricostruire l'origine, l'acquisizione, l'identificazione e le successive operazioni effettuate sulle evidenze.

ALLEGATO 6

MODELLO DI PIANO DI AZIONI CORRETTIVE

Non conformità Causa Correzione Responsabile Termine Verifica

APPROVAZIONE

Il presente Manuale è sottoposto all'approvazione dell'organo competente del SIPSE.

Codice: SIPSE-CCJC-MAN-03/2026
Versione: 1.0
Data: 13 novembre 2026

Organo approvante: _____

Presidente o rappresentante autorizzato: _____

Firma: _____

Cancelleria Generale: _____

Firma: _____