S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

Cancelleria Generale e Segreteria Tecnica per l'Effettività e la Conformità dei Diritti

DISCIPLINARE GENERALE CCJC

Regolamento per l'istituzione, il rilascio, la gestione e la sorveglianza della Certificazione di Conformità ai criteri giuridici, ai principi dello Jus Cogens e agli standard SIPSE

Codice normativo: SIPSE-CCJC-REG-01
Versione: 1.0
Settore iniziale: Imprese digitali, infrastrutture informatiche, intelligenza artificiale e piattaforme di servizi telematici.
Organo amministrativo: Cancelleria Generale SIPSE.
Organo tecnico: Segreteria Tecnica CCJC.

CAPO I – ISTITUZIONE, NATURA E FINALITÀ

Art. 1 – Istituzione della certificazione

1. Il Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE) istituisce la Certificazione di Conformità ai criteri giuridici, ai principi dello Jus Cogens e agli standard SIPSE, identificata dalla sigla CCJC.
2. La CCJC è uno strumento volontario di valutazione, attestazione e monitoraggio della conformità di imprese, organizzazioni, infrastrutture, prodotti, processi e servizi.
3. La certificazione è amministrata dalla Cancelleria Generale SIPSE attraverso una Segreteria Tecnica dedicata e un Comitato di Valutazione indipendente.
4. Il sistema è aperto a soggetti economici, organizzazioni, cooperative, sviluppatori, gestori di infrastrutture e operatori tecnologici, senza discriminazioni fondate sulla nazionalità o sulla forma giuridica.
5. Il presente Disciplinare costituisce il regolamento generale dello schema di certificazione SIPSE e può essere integrato da protocolli tecnici settoriali.

Art. 2 – Fondamento giuridico

1. La CCJC si fonda sui principi di dignità umana, autodeterminazione dei popoli, libertà economica, responsabilità sociale, legalità, trasparenza, buona fede e tutela dei diritti fondamentali.
2. Sono utilizzati, secondo il rispettivo ambito di applicazione:
   a. Carta delle Nazioni Unite;
   b. Dichiarazione universale dei diritti umani;
   c. Patto internazionale sui diritti civili e politici;
   d. Patto internazionale sui diritti economici, sociali e culturali;
   e. Convenzione di Vienna sul diritto dei trattati;
   f. norme imperative del diritto internazionale generale;
   g. convenzioni internazionali pertinenti;
   h. normativa europea e nazionale applicabile;
   i. standard tecnici internazionali pertinenti.
3. Il riferimento allo Jus Cogens non costituisce dichiarazione di conformità universale a tutte le norme imperative del diritto internazionale, ma comporta l'esame dei principi pertinenti all'attività sottoposta a valutazione.
4. La valutazione deve indicare le fonti giuridiche effettivamente applicabili, la loro natura e il rapporto con le attività esaminate.

Art. 3 – Natura ed effetti della certificazione

1. La CCJC costituisce un'attestazione documentale rilasciata dal SIPSE nell'ambito del proprio schema volontario.
2. La certificazione documenta:
   a. l'identità del soggetto certificato;
   b. il servizio o l'infrastruttura sottoposta a valutazione;
   c. i requisiti esaminati;
   d. le evidenze raccolte;
   e. il risultato dell'esame;
   f. il periodo di validità;
   g. gli eventuali limiti e condizioni.
3. La certificazione può essere utilizzata dal titolare nei rapporti commerciali, contrattuali, organizzativi e istituzionali, nel rispetto della normativa applicabile.
4. Non costituisce autorizzazione pubblica, licenza amministrativa, immunità giurisdizionale, esenzione normativa o protezione automatica contro sanzioni, provvedimenti giudiziari o misure delle autorità competenti.
5. Non sostituisce certificazioni obbligatorie, autorizzazioni, accreditamenti o verifiche previste dalle legislazioni applicabili.

Art. 4 – Finalità

Il sistema CCJC persegue le seguenti finalità:

1. Promuovere la responsabilità giuridica e tecnologica delle imprese.
2. Rendere verificabili gli impegni di conformità assunti dagli operatori economici.
3. Proteggere l'integrità documentale e la tracciabilità delle attività digitali.
4. Favorire la trasparenza dei sistemi algoritmici e delle infrastrutture.
5. Tutelare la riservatezza, la sicurezza e i diritti degli utenti.
6. Favorire l'interoperabilità fra sistemi economici, tecnologici e istituzionali.
7. Promuovere la cooperazione volontaria tra imprese, popoli e organizzazioni aderenti al SIPSE.

CAPO II – ORGANIZZAZIONE E COMPETENZE

Art. 5 – Organi competenti

Sono istituiti:

1. Cancelleria Generale SIPSE.
2. Segreteria Tecnica CCJC.
3. Comitato Indipendente di Valutazione.
4. Registro Generale delle Certificazioni SIPSE.
5. Collegio di Garanzia e Ricorso.
6. Infrastruttura tecnica SIPSE-IEMV per la registrazione e la verifica crittografica.

Art. 6 – Cancelleria Generale

La Cancelleria Generale:

1. riceve e protocolla le domande;
2. assegna il numero identificativo delle pratiche;
3. verifica la completezza amministrativa;
4. emette i certificati sulla base della decisione del Comitato;
5. gestisce il registro pubblico;
6. conserva il fascicolo documentale;
7. cura le notificazioni e le comunicazioni ufficiali;
8. amministra il sistema di rinnovo e aggiornamento dei titoli.

Art. 7 – Segreteria Tecnica

La Segreteria Tecnica:

1. esamina la documentazione presentata;
2. definisce il perimetro della verifica;
3. predispone il piano di valutazione;
4. individua gli esperti e gli auditor competenti;
5. raccoglie e analizza le evidenze;
6. redige il rapporto istruttorio;
7. formula una proposta motivata al Comitato di Valutazione;
8. gestisce il monitoraggio tecnico e le verifiche periodiche.

La Segreteria non può deliberare autonomamente il rilascio di una certificazione quando abbia svolto l'istruttoria della medesima pratica.

Art. 8 – Comitato Indipendente di Valutazione

1. Il Comitato è composto da almeno tre membri con competenze giuridiche, informatiche, economiche o di sicurezza digitale.
2. I membri dichiarano preventivamente eventuali conflitti d'interesse.
3. Il Comitato esamina il rapporto istruttorio e adotta una decisione motivata.
4. Può deliberare:
   a. approvazione;
   b. approvazione condizionata, nei limiti previsti dallo schema;
   c. richiesta di integrazione;
   d. sospensione dell'istruttoria;
   e. diniego.
5. Il componente che abbia un interesse personale, professionale o economico nella pratica deve astenersi.
6. La decisione deve essere registrata e sottoscritta secondo le procedure del SIPSE.

Art. 9 – Collegio di Garanzia

1. È istituito un Collegio distinto dagli organi di istruttoria e decisione.
2. Il Collegio esamina i reclami contro irregolarità procedurali, violazioni dell'imparzialità e decisioni contestate.
3. Il ricorso è presentato entro trenta giorni dalla comunicazione della decisione.
4. Il Collegio può confermare, annullare o rinviare la decisione per una nuova valutazione.
5. Il ricorso non impedisce l'accesso agli strumenti di tutela previsti dalla legge applicabile.

CAPO III – REQUISITI DI ACCESSO E AMBITO DELLA VALUTAZIONE

Art. 10 – Soggetti ammessi

Possono presentare domanda:

a. imprese individuali e società commerciali;
b. cooperative e consorzi;
c. organizzazioni e associazioni;
d. sviluppatori indipendenti;
e. fornitori di servizi cloud e hosting;
f. gestori di data center e infrastrutture informatiche;
g. piattaforme digitali e motori di ricerca;
h. sviluppatori e fornitori di sistemi di intelligenza artificiale;
i. gestori di protocolli e reti digitali;
j. operatori di commercio elettronico e servizi telematici.

Art. 11 – Ambito oggettivo

La certificazione può riguardare:

1. l'intera organizzazione;

2. una specifica unità operativa;
3. un prodotto digitale;
4. un servizio telematico;
5. un'infrastruttura informatica;
6. un sistema di intelligenza artificiale;
7. un processo di gestione dei dati;
8. un protocollo tecnologico;
9. un sistema documentale e contrattuale.

Il certificato deve identificare con precisione il perimetro valutato. Non è consentito estendere automaticamente la certificazione a prodotti, società controllate o servizi non esaminati.

Art. 12 – Requisiti generali

Il richiedente deve:

1. dimostrare la propria identità e l'esistenza giuridica, ove applicabile;
2. identificare il legale rappresentante o il responsabile autorizzato;
3. descrivere il servizio e la sua architettura;
4. dichiarare le giurisdizioni nelle quali opera;
5. presentare le politiche di sicurezza e gestione dei dati;
6. dichiarare eventuali procedimenti o incidenti rilevanti, nei limiti consentiti dalla legge;
7. accettare le procedure di verifica;
8. fornire informazioni veritiere e aggiornate.

Art. 13 – Obblighi del titolare

Il titolare si impegna a:

a. mantenere la conformità ai requisiti certificati;
b. comunicare le modifiche sostanziali dell'infrastruttura;
c. segnalare incidenti rilevanti;
d. collaborare alle verifiche di sorveglianza;
e. non utilizzare il marchio in modo ingannevole;
f. non presentare la certificazione come immunità o autorizzazione pubblica;
g. conservare le evidenze documentali;
h. rispettare gli obblighi di riservatezza e protezione dei dati;
i. consentire verifiche ragionevoli e proporzionate.

CAPO IV – CRITERI DI CONFORMITÀ

Art. 14 – Aree di valutazione

La valutazione CCJC è articolata nelle seguenti aree:

A. Conformità giuridica

- rispetto dei diritti fondamentali;
- correttezza contrattuale;
- trasparenza delle condizioni di servizio;
- rispetto delle norme imperative pertinenti;
- individuazione delle giurisdizioni applicabili.

B. Protezione dei dati

- base giuridica del trattamento;
- trasparenza informativa;
- minimizzazione dei dati;
- controllo degli accessi;
- conservazione e cancellazione;
- gestione delle richieste degli interessati.

C. Sicurezza informatica

- autenticazione;
- gestione delle credenziali;
- protezione dei sistemi;
- gestione delle vulnerabilità;
- continuità operativa;
- registrazione degli incidenti.

D. Trasparenza tecnologica

- documentazione dei processi;
- gestione delle modifiche;
- tracciabilità delle decisioni;
- identificazione dei responsabili;
- documentazione degli algoritmi, ove pertinente.

E. Integrità economica e commerciale

- trasparenza dei prezzi;
- condizioni contrattuali;
- gestione dei reclami;
- assenza di pratiche ingannevoli;
- tutela degli utenti e dei consumatori.

F. Responsabilità e diritti digitali

- libertà di espressione nel rispetto della legge;
- non discriminazione;
- tutela della dignità umana;
- procedure trasparenti di moderazione;
- diritto di contestazione e revisione delle decisioni automatizzate, ove applicabile.

Art. 15 – Metodo di valutazione

1. Ogni area è valutata attraverso documentazione, interviste, controlli tecnici, test e audit proporzionati al rischio.
2. Ogni requisito è classificato:
    - conforme;
    - parzialmente conforme;
    - non conforme;
    - non applicabile.
3. Le non conformità sono classificate come:
    - critiche;
    - maggiori;
    - minori.
4. Le non conformità critiche impediscono il rilascio.
5. Le non conformità maggiori richiedono correzione e nuova verifica prima del rilascio.
6. Le non conformità minori possono essere oggetto di piano correttivo con scadenza definita.
7. Ogni valutazione deve essere accompagnata da evidenze verificabili e da una motivazione.

CAPO V – PROCEDURA DI RILASCIO

Art. 16 – Presentazione dell'istanza

1. Il richiedente trasmette alla Cancelleria il Modulo CCJC-01.
2. La domanda deve contenere:
   a. dati identificativi;
   b. documentazione societaria o identificativa;
   c. descrizione del servizio;
   d. perimetro della certificazione;
   e. documentazione tecnica;
   f. dichiarazione di accettazione del Disciplinare;
   g. autorizzazione alle verifiche previste.
3. La Cancelleria rilascia ricevuta e numero di pratica.

Art. 17 – Istruttoria

1. Entro cinque giorni lavorativi la Segreteria verifica la completezza formale.
2. In caso di carenze, richiede un'integrazione.
3. Il richiedente dispone ordinariamente di trenta giorni per integrare la documentazione.
4. Completata l'istruttoria preliminare, è predisposto il piano di audit.
5. Il termine ordinario per la valutazione è di trenta giorni lavorativi dalla disponibilità della documentazione completa, salvo complessità tecnica, necessità di verifiche ulteriori o sospensioni motivate.

Art. 18 – Decisione e rilascio

1. Il Comitato esamina il rapporto finale.
2. In caso di esito positivo, la Cancelleria emette:
   a. Certificato CCJC;
   b. Rapporto sintetico di conformità;

c. Attestato di deposito crittografico;
d. Licenza d'uso del marchio CCJC;
e. identificativo pubblico di verifica.

3. Il rilascio è subordinato al completamento degli adempimenti amministrativi ed economici previsti dal tariffario.
4. Il diniego deve essere motivato e notificato al richiedente.

Art. 19 – Validità e rinnovo

1. La certificazione ha validità ordinaria di dodici mesi.
2. Il rinnovo è subordinato a una verifica di sorveglianza.
3. La domanda di rinnovo deve essere presentata almeno sessanta giorni prima della scadenza.
4. Il titolare deve comunicare ogni modifica sostanziale che possa compromettere i requisiti certificati.
5. Il rinnovo non è automatico.

CAPO VI – REGISTRO, SICUREZZA E DEPOSITO CRITTOGRAFICO

Art. 20 – Registro Generale CCJC

1. È istituito il Registro Generale delle Certificazioni SIPSE.
2. Ogni certificato riceve un codice univoco.
3. Il Registro contiene:
    - numero identificativo;
    - denominazione del titolare;
    - settore;
    - ambito certificato;
    - data di emissione;
    - data di scadenza;
    - stato della certificazione;
    - versione del disciplinare applicata.
4. Sono pubblicate esclusivamente le informazioni autorizzate e compatibili con la protezione dei dati e dei segreti commerciali.
5. Il Registro deve consentire la verifica dell'autenticità e dello stato del certificato.

Art. 21 – Deposito crittografico

1. I documenti ufficiali possono essere sottoposti a calcolo dell'impronta crittografica SHA-256.
2. Il deposito può essere effettuato mediante infrastruttura SIPSE-IEMV e registro distribuito multi-firma.
3. Sono registrati:
a. identificativo del documento;
b. impronta SHA-256;
c. data e ora della registrazione;

d. versione;
e. soggetto autorizzato alla registrazione;
f. riferimento alla transazione o al registro.

4. I dati personali, i codici sorgente e i documenti riservati non sono pubblicati sulla blockchain.
5. La marcatura crittografica dimostra la corrispondenza del documento con l'impronta registrata e contribuisce a documentarne l'esistenza e la sequenza temporale. Non prova autonomamente la veridicità del contenuto, la titolarità dei diritti o l'opponibilità universale del documento.

Art. 22 – Firma e autenticazione

1. I certificati devono essere sottoscritti mediante sistemi di firma idonei a identificare il soggetto emittente e a proteggere l'integrità del documento.
2. Ove siano richiesti effetti giuridici specifici nell'Unione europea o in altri ordinamenti, si utilizzano i sistemi di firma e validazione conformi alle rispettive disposizioni applicabili.
3. Il SIPSE conserva i dati di verifica e le evidenze di emissione.

CAPO VII – SORVEGLIANZA, SOSPENSIONE E REVOCA

Art. 23 – Sorveglianza

1. Il titolare è sottoposto a verifiche periodiche.
2. La sorveglianza ordinaria avviene almeno una volta ogni sei mesi.
3. Possono essere disposti audit straordinari in caso di:
   a. incidenti di sicurezza;
   b. modifiche sostanziali;
   c. reclami fondati;
   d. segnalazioni documentate;
   e. perdita dei requisiti certificati.

Art. 24 – Sospensione

La certificazione può essere sospesa in caso di:

1. perdita temporanea di requisiti essenziali;
2. mancata collaborazione agli audit;
3. dichiarazioni inesatte o incomplete rilevanti;
4. utilizzo improprio del marchio;
5. mancata attuazione delle misure correttive;
6. rischio concreto per gli utenti o per l'integrità del sistema certificato.

La sospensione deve essere motivata, notificata e registrata.

Art. 25 – Revoca

1. La revoca è deliberata dal Comitato in presenza di violazioni gravi o reiterate.
2. Il titolare ha diritto al contraddittorio, salvo misure cautelari urgenti e proporzionate.
3. La revoca determina la cessazione del diritto di utilizzare il marchio CCJC.
4. Lo stato del certificato viene aggiornato nel Registro.

Art. 26 – Reclami e ricorsi

1. Gli utenti e i soggetti interessati possono presentare segnalazioni documentate.
2. Il titolare può presentare ricorso contro sospensione, diniego o revoca.
3. Le procedure devono assicurare imparzialità, riservatezza e tracciabilità.
4. Gli esiti dei ricorsi sono registrati nel fascicolo.

CAPO VIII – AMMINISTRAZIONE ECONOMICA E RESPONSABILITÀ

Art. 27 – Tariffario

1. Il SIPSE adotta un tariffario pubblico.
2. Le tariffe possono differenziarsi in base a:
   a. dimensione dell'organizzazione;
   b. complessità del servizio;
   c. numero di sistemi sottoposti a verifica;
   d. livello di audit richiesto;
   e. costi di sorveglianza.
3. Sono previste condizioni agevolate per microimprese, cooperative, progetti di interesse sociale e organizzazioni senza scopo di lucro.
4. Il pagamento non determina il diritto automatico alla certificazione.
5. I costi di valutazione sono separati dalla decisione di conformità.

Art. 28 – Trasparenza finanziaria

1. Le entrate derivanti dalla CCJC sono contabilizzate separatamente.
2. Il SIPSE pubblica un rendiconto annuale delle attività di certificazione.
3. I compensi dei valutatori non possono dipendere dall'esito positivo della valutazione.
4. Sono vietati accordi economici che compromettano l'indipendenza degli organi.

Art. 29 – Responsabilità e limiti

1. Il SIPSE risponde delle attività amministrative e valutative nei limiti degli impegni assunti e delle norme applicabili.
2. Il certificato rappresenta una valutazione riferita a uno specifico ambito e a un determinato momento.
3. Il titolare conserva integralmente la propria responsabilità per le attività svolte e per gli obblighi previsti dalla legge.
4. Il SIPSE non garantisce l'assenza futura di violazioni, attacchi informatici, provvedimenti amministrativi o controversie.

CAPO IX – DISPOSIZIONI FINALI E ATTUAZIONE

Art. 30 – Entrata in vigore

Il presente Disciplinare entra in vigore secondo la deliberazione di approvazione dell'organo competente del SIPSE.

Art. 31 – Fase sperimentale

1. È istituita una fase sperimentale di novanta giorni.
2. Durante tale fase il SIPSE:
   a. costituisce gli organi di valutazione;
   b. approva le checklist;
   c. attiva il registro;
   d. realizza il sistema di verifica;
   e. sperimenta il deposito crittografico;
   f. seleziona un primo gruppo di richiedenti volontari;
   g. verifica la sostenibilità economica e organizzativa.
3. I titoli rilasciati nella fase sperimentale sono identificati come certificazioni pilota e non possono essere presentati come accreditamenti pubblici o certificazioni riconosciute da autorità terze.

Art. 32 – Revisione

Il Disciplinare è sottoposto a revisione almeno annuale, anche sulla base dell'evoluzione normativa, tecnologica e degli esiti delle verifiche.

Art. 33 – Clausola di salvaguardia

Il presente sistema è volontario e complementare agli ordinamenti giuridici applicabili. Nessuna disposizione può essere interpretata come autorizzazione a violare norme imperative, sottrarsi a obblighi legali o ostacolare legittime attività delle autorità competenti.

S.I.P.S.E. – Cancelleria Generale

Sistema delle Istituzioni dei Popoli per la Sovranità Economica

PAX NON ABSENTIA BELLI SED PRAESENTIA IUSTITIAE