C.I.A.P. – S.I.P.S.E.

CORTE INTERNAZIONALE PER L'AUTODETERMINAZIONE DEI POPOLI

INTERNATIONAL COURT FOR THE SELF-DETERMINATION OF PEOPLES

Venezia – Palazzo Ducale | Ginevra

PROTOCOLLO INTERNAZIONALE N. 04/2026

PER LA PROTEZIONE PREVENTIVA DEI POPOLI, DEI TESTIMONI, DEI RAPPRESENTANTI, DEI DIFENSORI DEI DIRITTI E DEI SEGNALANTI

Istituzione del Sistema di Allerta e Protezione Preventiva C.I.A.P. (SAP-CIAP)

Atto n. 04/2026 – Versione 1.0
Data: 11 novembre 2026
Classificazione: Protocollo istituzionale e procedurale
Ambito: Autodeterminazione dei popoli, diritti umani, protezione delle persone e prevenzione delle ritorsioni.

Motto istituzionale

PAX NON ABSENTIA BELLI SED PRAESENTIA IUSTITIAE

PREAMBOLO

La C.I.A.P. – Corte Internazionale per l'Autodeterminazione dei Popoli, nell'ambito della propria attività istituzionale, scientifica, consultiva e di promozione della tutela dei diritti dei popoli,

PREMESSO CHE

- la dignità umana, la vita, la libertà personale e la sicurezza costituiscono valori fondamentali dell'ordinamento internazionale dei diritti umani;
- il diritto dei popoli all'autodeterminazione è riconosciuto dall'articolo 1 comune al Patto internazionale sui diritti civili e politici e al Patto internazionale sui diritti economici, sociali e culturali;

- la Carta delle Nazioni Unite, la Dichiarazione universale dei diritti umani e gli strumenti internazionali applicabili impongono agli Stati obblighi di tutela secondo le rispettive disposizioni;
- i rappresentanti dei popoli, i difensori dei diritti umani, i giornalisti, i ricercatori, i testimoni e coloro che segnalano violazioni possono essere esposti a minacce, intimidazioni, discriminazioni, ritorsioni o altre forme di pressione;
- la Dichiarazione delle Nazioni Unite sui difensori dei diritti umani del 1998 riconosce il diritto di promuovere e proteggere i diritti umani e le libertà fondamentali;
- la protezione delle fonti, la riservatezza delle informazioni, l'integrità delle testimonianze e la sicurezza dei segnalanti rappresentano condizioni essenziali per l'accertamento e la documentazione delle violazioni;
- la prevenzione delle ritorsioni costituisce un elemento fondamentale per garantire la partecipazione libera e consapevole delle persone ai procedimenti di tutela dei diritti;

CONSIDERATO CHE

la tutela dell'autodeterminazione dei popoli non può essere effettiva se coloro che esercitano pacificamente tale diritto sono esposti a intimidazioni, minacce o discriminazioni;

la protezione preventiva deve essere organizzata attraverso procedure verificabili, proporzionate, indipendenti e rispettose delle competenze delle autorità nazionali e internazionali;

è necessario distinguere la raccolta e la valutazione istituzionale delle segnalazioni dalle attività di indagine, dalle misure di protezione coercitiva e dalle decisioni giudiziarie riservate agli organi competenti;

ADOTTA, quale testo istituzionale sottoposto all'approvazione degli organi competenti, il seguente Protocollo.

TITOLO I – DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente Protocollo disciplina il sistema interno C.I.A.P. di prevenzione, ricezione, classificazione, documentazione e monitoraggio delle segnalazioni concernenti minacce, intimidazioni, ritorsioni o situazioni di rischio nei confronti dei soggetti tutelati.
2. Il Protocollo istituisce il Sistema di Allerta e Protezione Preventiva C.I.A.P., di seguito denominato **SAP-CIAP**.
3. Il sistema ha natura preventiva, documentale, istituzionale e di raccordo.
4. Le attività previste non sostituiscono le competenze delle autorità giudiziarie, amministrative, diplomatiche o di polizia degli Stati né quelle delle organizzazioni internazionali competenti.

Articolo 2 – Finalità

Il Protocollo persegue le seguenti finalità:

a. prevenire e documentare situazioni di rischio;

b. proteggere la riservatezza e l'integrità delle persone segnalanti;

c. favorire la conservazione delle prove e delle informazioni;

d. contrastare le ritorsioni connesse all'esercizio pacifico dei diritti;

e. promuovere l'accesso alle procedure di tutela nazionali e internazionali;

f. garantire la tracciabilità delle segnalazioni;

g. sviluppare una metodologia uniforme di valutazione del rischio;

h. promuovere la cooperazione volontaria con soggetti e istituzioni competenti;

i. formulare raccomandazioni preventive e richieste di attenzione istituzionale nei limiti delle competenze disponibili.

Articolo 3 – Principi fondamentali

Il SAP-CIAP opera nel rispetto dei seguenti principi:

1. centralità della persona e dignità umana;
2. legalità e rispetto delle fonti internazionali applicabili;
3. indipendenza e imparzialità;
4. prevenzione del danno;
5. riservatezza e protezione dei dati;
6. consenso informato;
7. non discriminazione;
8. proporzionalità;
9. precauzione;
10. presunzione di buona fede del segnalante, salva verifica;
11. accuratezza documentale;
12. divieto di strumentalizzazione politica;
13. tutela del contraddittorio e dei diritti delle persone coinvolte;
14. rispetto delle competenze delle autorità legittimamente preposte.

Articolo 4 – Natura e limiti del Protocollo

1. Il presente Protocollo costituisce uno strumento di disciplina istituzionale interna della C.I.A.P.
2. La sua adozione non determina automaticamente il riconoscimento internazionale della C.I.A.P., l'attribuzione di personalità giuridica internazionale, l'istituzione di una giurisdizione obbligatoria o il conferimento di immunità.
3. Il SAP-CIAP non esercita poteri di polizia, arresto, perquisizione, sorveglianza coercitiva, protezione armata o imposizione di misure nei confronti di Stati e terzi.
4. Ogni attività di cooperazione esterna è subordinata alla disponibilità di un valido titolo giuridico, al consenso delle parti interessate e al rispetto della legislazione applicabile.

5. Le eventuali competenze giurisdizionali vincolanti della C.I.A.P. potranno derivare esclusivamente da un futuro strumento convenzionale validamente concluso ed entrato in vigore per le parti interessate.

Articolo 5 – Definizioni

Ai fini del presente Protocollo si intende per:

a. **persona protetta:** soggetto ammesso alle procedure di tutela del SAP-CIAP;

b. **segnalante:** persona fisica o organizzazione che comunica informazioni su una possibile violazione o situazione di rischio;

c. **testimone:** persona che dichiara di possedere conoscenze dirette o indirette rilevanti;

d. **rappresentante:** persona che agisce legittimamente per conto di un popolo, comunità o organizzazione;

e. **difensore dei diritti:** persona che promuove pacificamente i diritti umani e l'autodeterminazione;

f. **ritorsione:** condotta pregiudizievole collegata alla segnalazione, alla testimonianza o all'esercizio pacifico di un diritto;

g. **rischio imminente:** situazione nella quale elementi concreti indicano la possibilità di un danno grave in tempi ravvicinati;

h. **fascicolo protetto:** insieme organizzato delle informazioni riservate relative a una segnalazione;

i. **misura preventiva:** iniziativa non coercitiva volta a ridurre l'esposizione a un rischio o a facilitare l'accesso alle autorità competenti.

TITOLO II – SOGGETTI BENEFICIARI DELLA PROTEZIONE

Articolo 6 – Ambito soggettivo

Possono richiedere l'attivazione del SAP-CIAP:

1. popoli e comunità che esercitano pacificamente il diritto all'autodeterminazione;
2. rappresentanti e delegati di popoli;
3. testimoni e persone informate sui fatti;
4. difensori dei diritti umani;
5. ricercatori, studiosi e documentaristi;
6. giornalisti e operatori dell'informazione;
7. segnalanti di presunte violazioni dei diritti fondamentali;
8. familiari e collaboratori esposti a rischi direttamente connessi alle attività di cui sopra;

9. mediatori e osservatori impegnati in iniziative pacifiche di tutela dei diritti.

Articolo 7 – Accesso senza discriminazioni

1. L'accesso alle procedure non può essere negato per ragioni di nazionalità, origine, lingua, appartenenza culturale, condizione economica, opinione politica o orientamento istituzionale.
2. La tutela non è subordinata all'adesione alla C.I.A.P. o al S.I.P.S.E.
3. Non è richiesta la condivisione delle posizioni politiche, culturali o istituzionali della C.I.A.P.
4. La valutazione deve fondarsi su elementi pertinenti e verificabili.

Articolo 8 – Protezione delle comunità e dei popoli

1. Il SAP-CIAP può ricevere segnalazioni riguardanti rischi collettivi che interessino un popolo o una comunità.
2. La valutazione considera la possibile natura sistematica, discriminatoria o generalizzata delle condotte.
3. Le segnalazioni collettive devono individuare, ove possibile, i soggetti interessati, il territorio, il periodo temporale e le condotte denunciate.
4. La protezione collettiva non comporta il riconoscimento automatico di uno status statuale o di una rappresentanza esclusiva.

Articolo 9 – Soggetti vulnerabili

1. È assicurata particolare attenzione ai minori, alle persone con disabilità, agli anziani e a coloro che si trovino in condizioni di particolare vulnerabilità.
2. Le segnalazioni riguardanti minori sono trattate secondo il principio del superiore interesse del minore e le garanzie previste dalle norme applicabili.
3. La raccolta delle informazioni deve evitare ogni forma di vittimizzazione secondaria.

Articolo 10 – Divieto di abuso della protezione

1. Il sistema non può essere utilizzato per intimidire terzi, diffondere accuse consapevolmente false, perseguire finalità di propaganda o ottenere vantaggi estranei alle finalità del Protocollo.
2. La contestazione della buona fede richiede elementi concreti e una valutazione imparziale.
3. Nessuna misura può essere adottata esclusivamente sulla base di una divergenza politica o istituzionale.

TITOLO III – SISTEMA DI ALLERTA E PROTEZIONE PREVENTIVA

Articolo 11 – Istituzione del SAP-CIAP

1. È istituito il **Sistema di Allerta e Protezione Preventiva C.I.A.P. (SAP-CIAP)**.
2. Il sistema costituisce la struttura organizzativa preposta alla ricezione, classificazione, gestione e monitoraggio delle segnalazioni.
3. Il SAP-CIAP opera attraverso procedure documentate e personale formalmente incaricato.
4. L'attivazione del sistema non costituisce accertamento definitivo della veridicità delle accuse.

Articolo 12 – Funzioni

Il SAP-CIAP svolge le seguenti funzioni:

a. ricezione delle segnalazioni;

b. registrazione e attribuzione di un codice identificativo;

c. verifica preliminare della completezza documentale;

d. valutazione del livello di rischio;

e. individuazione delle esigenze urgenti di tutela;

f. conservazione sicura delle informazioni;

g. monitoraggio dell'evoluzione del rischio;

h. predisposizione di rapporti riservati;

i. formulazione di raccomandazioni preventive;

j. eventuale raccordo con autorità e organizzazioni competenti.

Articolo 13 – Unità organizzative

Il SAP-CIAP si articola nelle seguenti unità funzionali:

1. **Unità di ricezione e registrazione:** acquisisce le segnalazioni.
2. **Unità di valutazione del rischio:** esamina gli elementi disponibili e formula la classificazione.
3. **Unità di protezione documentale:** cura la sicurezza e la conservazione dei fascicoli.
4. **Unità di raccordo istituzionale:** predispone le comunicazioni verso soggetti competenti.
5. **Unità di monitoraggio:** verifica l'evoluzione delle situazioni segnalate.
6. **Responsabile della protezione dei dati:** svolge le funzioni previste dalla normativa applicabile, ove formalmente designato.

Le unità possono essere organizzate in forma coordinata, nel rispetto della separazione delle funzioni.

Articolo 14 – Responsabile SAP-CIAP

1. Il Responsabile SAP-CIAP è nominato con atto formale.
2. Deve possedere comprovata competenza in materia di diritti umani, procedure documentali, gestione dei rischi o protezione dei dati.
3. Opera secondo criteri di indipendenza, riservatezza e imparzialità.
4. Non può intervenire in una valutazione nella quale sussista un conflitto di interessi.
5. Presenta periodicamente una relazione riservata sull'attività svolta.

Articolo 15 – Registro delle segnalazioni

1. Ogni segnalazione ammessa alla trattazione è iscritta in un registro riservato.
2. A ciascun fascicolo è assegnato un codice univoco.
3. Il registro riporta almeno:
    - data e modalità di ricezione;
    - oggetto della segnalazione;
    - soggetti interessati, ove identificabili;
    - classificazione preliminare;
    - responsabile incaricato;
    - misure documentali adottate;
    - aggiornamenti e conclusione della procedura.
4. Il registro è accessibile esclusivamente ai soggetti autorizzati.

TITOLO IV – RICEZIONE E VERIFICA DELLE SEGNALAZIONI

Articolo 16 – Modalità di presentazione

1. Le segnalazioni possono essere presentate mediante canali istituzionali formalmente attivati.
2. Possono essere trasmesse in forma scritta, documentale o attraverso modalità digitali sicure.
3. Sono ammesse segnalazioni presentate da rappresentanti o delegati, purché sia chiarita la loro legittimazione.
4. Le segnalazioni anonime possono essere prese in considerazione quando contengano elementi specifici e verificabili.

Articolo 17 – Contenuto minimo

La segnalazione dovrebbe contenere, ove disponibili:

a. descrizione dei fatti;

b. data e luogo degli eventi;

c. soggetti coinvolti;

d. natura del rischio;

e. eventuali minacce o condotte ritorsive;

f. documenti e materiali disponibili;

g. autorità eventualmente già informate;

h. indicazione delle esigenze urgenti di tutela;

i. recapito sicuro per eventuali comunicazioni.

La mancanza di uno o più elementi non determina automaticamente l'inammissibilità.

Articolo 18 – Ricezione e conferma

1. La ricezione è registrata con data certa, ove tecnicamente possibile.
2. Il segnalante riceve un codice identificativo e una conferma di ricezione, quando esiste un recapito sicuro.
3. La conferma non equivale ad accoglimento, riconoscimento della fondatezza o attribuzione di uno status protetto.
4. Le comunicazioni devono evitare di esporre il segnalante a ulteriori rischi.

Articolo 19 – Valutazione preliminare

La valutazione preliminare verifica:

1. la riconducibilità della segnalazione alle finalità del Protocollo;
2. la presenza di elementi sufficientemente specifici;
3. l'esistenza di un rischio attuale o potenziale;
4. l'eventuale necessità di interventi urgenti da parte delle autorità competenti;
5. la disponibilità di documentazione;
6. la necessità di ulteriori informazioni;
7. l'eventuale presenza di conflitti di interesse o ragioni di astensione.

Articolo 20 – Verifica delle informazioni

1. Le informazioni sono sottoposte a verifica di coerenza, provenienza e attendibilità.
2. Si distinguono chiaramente:
    - fatti documentati;
    - dichiarazioni testimoniali;
    - informazioni indirette;
    - elementi non verificati;
    - valutazioni e inferenze.
3. Non è consentito presentare come accertato ciò che risulta soltanto dichiarato o ipotizzato.
4. La verifica non costituisce indagine giudiziaria né sostituisce l'accertamento delle autorità competenti.

Articolo 21 – Contraddittorio e tutela delle persone coinvolte

1. Le persone o istituzioni oggetto di una segnalazione non sono considerate responsabili per il solo fatto di essere menzionate.
2. La diffusione di accuse non verificate è vietata.
3. Qualora sia prevista una valutazione istituzionale non urgente, può essere richiesto un chiarimento alla persona o al soggetto interessato, quando ciò sia compatibile con la sicurezza del segnalante.
4. Il contraddittorio non deve essere attivato in modo da esporre la persona segnalante a ritorsioni o pericoli.
5. La riservatezza e il diritto di difesa devono essere bilanciati secondo le circostanze e le norme applicabili.

TITOLO V – CLASSIFICAZIONE E VALUTAZIONE DEL RISCHIO

Articolo 22 – Principio di valutazione preventiva

1. Ogni segnalazione rilevante può essere sottoposta a valutazione preventiva del rischio.
2. La valutazione deve essere individualizzata, documentata e aggiornata.
3. La classificazione è uno strumento interno di gestione e non costituisce dichiarazione giudiziaria di responsabilità.

Articolo 23 – Livelli di rischio

Sono istituiti cinque livelli:

Livello 0 – Ordinario

Non emergono elementi concreti di rischio, pur restando possibile la conservazione documentale della segnalazione.

Livello 1 – Attenzione

Sono presenti elementi di preoccupazione non ancora sufficienti a indicare una minaccia concreta.

Livello 2 – Significativo

Emergono condotte o circostanze che possono determinare pressioni, discriminazioni o ritorsioni.

Livello 3 – Elevato

Sono presenti elementi specifici indicativi di una possibile minaccia grave o di una situazione di rischio persistente.

Livello 4 – Critico o imminente

Emergono elementi concreti che indicano un possibile danno grave e temporalmente ravvicinato alla vita, all'integrità personale o alla libertà.

Articolo 24 – Indicatori di rischio

La valutazione può considerare:

a. specificità e credibilità della minaccia;

b. prossimità temporale;

c. precedenti episodi di intimidazione;

d. capacità e possibilità materiale del soggetto minacciante;

e. esposizione pubblica della persona;

f. vulnerabilità individuale;

g. eventuali ritorsioni già verificatesi;

h. diffusione di dati personali;

i. minacce rivolte a familiari o collaboratori;

j. contesto territoriale e istituzionale;

k. possibilità di accesso a misure di tutela pubbliche.

Articolo 25 – Matrice di valutazione

1. Il SAP-CIAP adotta una matrice di valutazione che distingue probabilità, gravità e imminenza.
2. Ogni indicatore deve essere accompagnato dalla relativa fonte documentale o dichiarativa.
3. La classificazione non può derivare esclusivamente da un punteggio automatico.
4. Il giudizio finale deve essere motivato da un operatore responsabile.

Articolo 26 – Riesame

1. La classificazione può essere modificata quando emergano nuovi elementi.
2. Le situazioni di livello 3 e 4 sono sottoposte a monitoraggio prioritario.
3. La persona interessata può richiedere il riesame della classificazione.
4. Il riesame deve essere effettuato, ove possibile, da un soggetto diverso da quello che ha adottato la valutazione iniziale.

TITOLO VI – MISURE PREVENTIVE E PROTEZIONE

Articolo 27 – Tipologia delle misure

Nel rispetto dei limiti del Protocollo, il SAP-CIAP può proporre o attivare, secondo le proprie effettive capacità organizzative:

1. misure di protezione documentale;
2. assistenza nella predisposizione di segnalazioni alle autorità competenti;
3. conservazione riservata delle informazioni;
4. raccomandazioni di sicurezza informativa;
5. monitoraggio delle ritorsioni;
6. supporto alla documentazione degli eventi;
7. comunicazioni istituzionali di attenzione;
8. facilitazione del contatto con organizzazioni competenti;
9. raccomandazioni per l'accesso a forme di assistenza legale o umanitaria;
10. misure di riduzione dell'esposizione pubblica, con il consenso dell'interessato.

Articolo 28 – Rischio imminente

1. In presenza di elementi indicativi di rischio imminente, il SAP-CIAP attribuisce priorità assoluta alla segnalazione.
2. La persona interessata è invitata, quando possibile, a contattare immediatamente i servizi pubblici di emergenza e le autorità territorialmente competenti.
3. Il SAP-CIAP può assistere nella predisposizione di una comunicazione urgente alle autorità o agli organismi competenti.
4. Il sistema non garantisce interventi fisici, protezione armata o soccorso immediato.
5. La segnalazione al SAP-CIAP non sostituisce la denuncia, la richiesta di protezione o l'attivazione dei servizi di emergenza.

Articolo 29 – Protezione della riservatezza

1. L'identità del segnalante è trattata con riservatezza.
2. L'identità non può essere comunicata a soggetti terzi senza una base giuridica valida o, ove richiesto, il consenso dell'interessato.
3. Sono previste limitazioni di accesso ai fascicoli secondo il principio della necessità di conoscenza.
4. La riservatezza può essere limitata soltanto nei casi previsti dalla legge e secondo criteri di necessità e proporzionalità.
5. La persona interessata deve essere informata, quando possibile e lecito, dei limiti applicabili alla riservatezza.

Articolo 30 – Protezione dei dati personali

1. Il trattamento dei dati personali deve rispettare la normativa applicabile, incluso il Regolamento (UE) 2016/679 quando applicabile.

2. Sono raccolti esclusivamente i dati adeguati, pertinenti e necessari alle finalità del Protocollo.
3. I dati relativi a salute, opinioni politiche, convinzioni religiose, appartenenza etnica o altre categorie particolari sono trattati soltanto in presenza di una valida base giuridica e delle garanzie previste.
4. Sono adottate misure tecniche e organizzative adeguate al rischio.
5. Devono essere stabiliti tempi di conservazione, procedure di cancellazione e modalità di esercizio dei diritti degli interessati.

Articolo 31 – Sicurezza informatica

Il SAP-CIAP adotta, in relazione alle risorse effettivamente disponibili:

a. autenticazione degli utenti autorizzati;

b. cifratura dei dati durante la trasmissione e, ove possibile, a riposo;

c. registrazione degli accessi;

d. copie di sicurezza protette;

e. separazione tra dati identificativi e documentazione del caso, ove tecnicamente possibile;

f. procedure di gestione degli incidenti;

g. verifica periodica dei sistemi;

h. limitazione dei privilegi di accesso.

Articolo 32 – Protezione delle testimonianze

1. Le testimonianze sono registrate in modo da preservarne integrità e provenienza.
2. Le dichiarazioni sono conservate nella loro formulazione originaria, ove possibile.
3. Ogni trascrizione o traduzione deve indicare il soggetto responsabile e la data dell'operazione.
4. Le modifiche successive devono essere tracciabili.
5. La testimonianza non può essere alterata, manipolata o utilizzata fuori dal contesto documentale senza adeguate garanzie.

Articolo 33 – Protezione contro le ritorsioni

1. Il SAP-CIAP riconosce particolare rilevanza alle condotte pregiudizievoli collegate alla segnalazione o alla testimonianza.
2. Le eventuali ritorsioni sono registrate come eventi autonomi e collegati al fascicolo originario.
3. La valutazione considera il rapporto temporale e causale tra attività del segnalante e condotta pregiudizievole.
4. Il sistema può formulare raccomandazioni e predisporre comunicazioni istituzionali, senza sostituirsi agli organi competenti.

Articolo 34 – Protezione dei familiari e dei collaboratori

La tutela può essere estesa, nei limiti del Protocollo e sulla base di elementi concreti, ai familiari e ai collaboratori direttamente esposti a rischi derivanti dall'attività del soggetto principale.

TITOLO VII – COMUNICAZIONI E COOPERAZIONE ISTITUZIONALE

Articolo 35 – Comunicazioni alle autorità competenti

1. Il SAP-CIAP può predisporre comunicazioni documentali indirizzate alle autorità nazionali o agli organismi internazionali competenti.
2. Le comunicazioni devono indicare la natura della segnalazione, gli elementi disponibili e il grado di verifica.
3. La comunicazione non può essere presentata come decisione giudiziaria o accertamento vincolante.
4. La trasmissione di dati personali richiede una base giuridica appropriata e il rispetto delle garanzie di riservatezza.

Articolo 36 – Cooperazione internazionale

La C.I.A.P. può promuovere forme di cooperazione volontaria con:

- organizzazioni internazionali;
- istituzioni nazionali per i diritti umani;
- organismi indipendenti;
- università e centri di ricerca;
- organizzazioni umanitarie;
- ordini e associazioni professionali;
- soggetti qualificati operanti nella tutela dei diritti.

La cooperazione è subordinata alle competenze effettive e alla disponibilità dei soggetti coinvolti.

Articolo 37 – Comunicazioni urgenti

1. Nei casi di livello 4 può essere predisposta una comunicazione urgente di allerta.
2. La comunicazione deve essere strettamente necessaria, proporzionata e documentata.
3. L'identità della persona interessata è comunicata soltanto quando indispensabile e giuridicamente consentito.
4. La comunicazione deve precisare che si tratta di una segnalazione preventiva e non di un accertamento definitivo.

Articolo 38 – Rapporti con le Nazioni Unite

1. Il SAP-CIAP può predisporre documentazione destinata ai meccanismi delle Nazioni Unite competenti in materia di diritti umani.
2. La trasmissione avviene attraverso i canali e le procedure ufficialmente previsti.
3. La C.I.A.P. non si attribuisce lo status di organo delle Nazioni Unite né la facoltà di impartire istruzioni ai relativi organismi.
4. Le comunicazioni devono rispettare i requisiti di ammissibilità, riservatezza e procedura previsti dal meccanismo destinatario.

Articolo 39 – Rapporti con gli organismi regionali

Il SAP-CIAP può predisporre documentazione per gli organismi regionali di tutela dei diritti umani, nel rispetto dei rispettivi strumenti istitutivi, requisiti di competenza e procedure.

Articolo 40 – Divieto di falsa rappresentazione istituzionale

È vietato:

a. presentare una comunicazione C.I.A.P. come provvedimento di un organo delle Nazioni Unite;

b. dichiarare l'esistenza di un mandato internazionale non effettivamente conferito;

c. attribuire a una segnalazione valore di sentenza;

d. utilizzare simboli o denominazioni di organizzazioni internazionali in modo idoneo a generare confusione;

e. dichiarare l'esistenza di misure di protezione non effettivamente attivate.

TITOLO VIII – GARANZIE PROCEDURALI E CONTROLLO

Articolo 41 – Indipendenza della valutazione

1. La valutazione delle segnalazioni deve essere indipendente da interessi politici, economici o personali.
2. I soggetti coinvolti in un conflitto di interessi devono dichiararlo e astenersi.
3. Ogni decisione interna deve essere motivata.
4. Nessun componente può modificare arbitrariamente una classificazione o sopprimere documenti.

Articolo 42 – Diritto di informazione

La persona segnalante ha diritto, nei limiti della riservatezza e della sicurezza:

a. di conoscere il codice identificativo del fascicolo;

b. di ricevere informazioni essenziali sullo stato della procedura;

c. di trasmettere ulteriori documenti;

d. di chiedere il riesame della classificazione;

e. di conoscere i limiti e le possibilità effettive del sistema.

Articolo 43 – Reclami

1. È ammesso reclamo contro omissioni, irregolarità procedurali o trattamenti non conformi al Protocollo.
2. Il reclamo è esaminato da un soggetto diverso, ove possibile, da quello responsabile dell'attività contestata.
3. Il reclamo non può determinare ritorsioni o penalizzazioni nei confronti del segnalante.
4. L'esito è comunicato in forma motivata, nel rispetto delle informazioni riservate.

Articolo 44 – Controllo interno

1. L'attività del SAP-CIAP è sottoposta a controllo periodico.
2. Il controllo verifica la correttezza procedurale, la sicurezza dei dati, la tracciabilità e il rispetto dei principi di imparzialità.
3. Le verifiche devono essere documentate.
4. Eventuali irregolarità sono sottoposte agli organi interni competenti.

Articolo 45 – Revisione indipendente

La C.I.A.P. può istituire un collegio di revisione indipendente incaricato di esaminare le procedure, formulare raccomandazioni e verificare il rispetto delle garanzie previste dal Protocollo.

TITOLO IX – RESPONSABILITÀ, TRASPARENZA E RENDICONTAZIONE

Articolo 46 – Responsabilità degli operatori

1. Gli operatori sono responsabili della corretta gestione delle informazioni e delle procedure loro affidate.
2. Sono vietati l'accesso non autorizzato, la divulgazione indebita, la manipolazione dei documenti e l'utilizzo dei dati per finalità estranee.
3. Le violazioni sono valutate secondo le norme interne applicabili e nel rispetto del contraddittorio.

Articolo 47 – Divieto di discriminazione e strumentalizzazione

Il SAP-CIAP non può essere utilizzato per discriminare, intimidire, screditare o delegittimare soggetti sulla base delle loro opinioni, appartenenze o posizioni istituzionali.

Articolo 48 – Trasparenza istituzionale

1. La C.I.A.P. può pubblicare rapporti aggregati sull'attività del SAP-CIAP.
2. I rapporti non devono contenere dati personali o elementi che consentano l'identificazione indiretta delle persone protette.
3. La trasparenza deve essere compatibile con la sicurezza dei soggetti coinvolti.

Articolo 49 – Relazione annuale

È prevista una relazione annuale contenente, in forma aggregata:

a. numero delle segnalazioni ricevute;

b. distribuzione per livello di rischio;

c. tipologia delle condotte segnalate;

d. tempi medi di trattamento;

e. numero delle richieste di riesame;

f. misure documentali e comunicazioni istituzionali effettuate;

g. criticità procedurali;

h. raccomandazioni di miglioramento.

Articolo 50 – Valutazione dell'efficacia

L'efficacia del SAP-CIAP è valutata sulla base di indicatori quali:

- tempestività nella ricezione;
- completezza della documentazione;
- qualità della valutazione;
- rispetto della riservatezza;
- tracciabilità delle procedure;
- correttezza delle comunicazioni;
- accessibilità del sistema;
- gestione delle richieste di riesame.

Nessun indicatore deve incentivare la classificazione artificiosamente elevata del rischio o la moltiplicazione delle segnalazioni.

TITOLO X – SVILUPPO CONVENZIONALE E DISPOSIZIONI FINALI

Articolo 51 – Collegamento con la futura Convenzione istitutiva

1. Il presente Protocollo costituisce una componente dell'architettura istituzionale e procedurale della C.I.A.P.
2. Esso potrà essere coordinato con la futura Convenzione multilaterale istitutiva della Corte.
3. La Convenzione potrà disciplinare, secondo il consenso degli Stati e degli altri soggetti legittimati a parteciparvi:
    - obblighi di cooperazione;
    - procedure di protezione dei testimoni;
    - garanzie per i rappresentanti dei popoli;
    - modalità di comunicazione e assistenza;
    - forme di tutela delle persone esposte a ritorsioni;
    - eventuali competenze giurisdizionali.
4. Le disposizioni future avranno efficacia esclusivamente secondo le regole di conclusione, entrata in vigore e applicazione previste dal diritto dei trattati.

Articolo 52 – Distinzione tra attività attuale e futura giurisdizione

1. Le attività attuali del SAP-CIAP hanno natura istituzionale, documentale, scientifica, preventiva e consultiva.
2. I rapporti, le valutazioni e le raccomandazioni non costituiscono sentenze internazionali vincolanti.
3. Eventuali competenze giudiziarie future saranno esercitate soltanto in presenza di un valido titolo convenzionale e nei limiti della giurisdizione accettata.
4. Nessuna disposizione del presente Protocollo può essere interpretata come attribuzione anticipata di competenze giudiziarie obbligatorie.

Articolo 53 – Clausola di salvaguardia dei diritti

Il presente Protocollo non limita né sostituisce i diritti e i rimedi riconosciuti dagli ordinamenti nazionali e internazionali. La persona interessata conserva il diritto di rivolgersi alle autorità e agli organismi competenti secondo le procedure applicabili.

Articolo 54 – Interpretazione conforme

Le disposizioni sono interpretate, per quanto applicabile, in conformità con:

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. Dichiarazione delle Nazioni Unite sui difensori dei diritti umani;

f. Convenzioni internazionali pertinenti;

g. norme applicabili in materia di protezione dei dati personali;

h. principi generali di legalità, imparzialità e proporzionalità.

Articolo 55 – Revisione del Protocollo

1. Il Protocollo è sottoposto a revisione periodica.
2. Le modifiche devono essere approvate dall'organo competente secondo le fonti istitutive della C.I.A.P.
3. Le modifiche non possono ridurre le garanzie fondamentali senza una motivazione giuridica e istituzionale adeguata.
4. Ogni versione deve essere identificata mediante numero, data e cronologia delle modifiche.

Articolo 56 – Entrata in vigore interna

1. Il presente Protocollo è sottoposto all'approvazione dell'organo competente della C.I.A.P.
2. La sua efficacia interna decorre dalla data di approvazione formalmente documentata.
3. L'effettiva operatività del SAP-CIAP è subordinata alla nomina dei responsabili, all'adozione delle procedure tecniche e alla disponibilità delle risorse necessarie.
4. Nessuna attività di protezione può essere dichiarata operativa prima che siano state predisposte le relative condizioni organizzative e di sicurezza.

ALLEGATO A

MODULO RISERVATO DI SEGNALAZIONE

Codice fascicolo: da assegnare
Data di ricezione: _____
Canale di ricezione: _____

1. Dati del segnalante

- Nome e cognome, se comunicati:
- Organizzazione o rappresentanza:
- Paese:
- Recapito sicuro:

- Modalità preferita di comunicazione:
- Richiesta di riservatezza: SÌ / NO

2. Natura della segnalazione

- Minaccia personale
- Intimidazione
- Ritorsione
- Discriminazione
- Minaccia a familiari o collaboratori
- Violazione dei diritti fondamentali
- Rischio collettivo
- Altro

3. Descrizione dei fatti

Data, luogo, circostanze, soggetti coinvolti e descrizione dettagliata.

4. Documentazione disponibile

- Documenti
- Comunicazioni
- Fotografie
- Registrazioni
- Testimonianze
- Altri elementi

5. Valutazione richiesta

- Ordinaria
- Prioritaria
- Urgente
- Rischio potenzialmente imminente

6. Dichiarazione

Il sottoscritto dichiara, per quanto a propria conoscenza, che le informazioni trasmesse sono veritiere e che gli elementi presentati sono stati indicati secondo la loro effettiva natura.

Data: _____

Firma, ove possibile: _____

ALLEGATO B

SCHEDA DI VALUTAZIONE DEL RISCHIO

Indicatore	Valutazione
Gravità potenziale	Bassa / Media / Alta / Critica
Probabilità	Bassa / Media / Alta
Imminenza	Non imminente / Prossima / Immediata
Vulnerabilità	Ordinaria / Elevata
Precedenti episodi	Assenti / Presenti / Documentati
Rischio per terzi	No / Possibile / Concreto
Attendibilità documentale	Limitata / Parziale / Significativa

Classificazione proposta: Livello 0 / 1 / 2 / 3 / 4

Motivazione: _____

Responsabile della valutazione: _____

Data del riesame: _____

ALLEGATO C

MODELLO DI COMUNICAZIONE URGENTE DI ALLERTA

C.I.A.P. – S.A.P.-C.I.A.P.
Comunicazione riservata n. _____

Oggetto: Segnalazione preventiva concernente una possibile situazione di rischio per l'incolumità o i diritti fondamentali di una persona o comunità.

La C.I.A.P., nell'ambito delle proprie attività istituzionali di documentazione, prevenzione e tutela dei diritti dei popoli, comunica di aver ricevuto una segnalazione concernente una possibile situazione di rischio.

La presente comunicazione:

1. ha natura preventiva e documentale;
2. non costituisce accertamento giudiziario definitivo;
3. non attribuisce responsabilità a soggetti non sottoposti a un procedimento competente;
4. è trasmessa affinché l'autorità destinataria possa valutare, nell'ambito delle proprie competenze, l'eventuale necessità di interventi;
5. tutela l'identità delle persone coinvolte nei limiti consentiti dalla legge.

Livello di rischio attribuito: _____

Elementi essenziali: _____

Richiesta istituzionale: valutazione della situazione e, ove ne ricorrano i presupposti, adozione delle misure di competenza.

Responsabile della comunicazione: _____

ALLEGATO D

REGISTRO DELLE MISURE PREVENTIVE

Codice	Data	Livello	Misura documentale	Responsabile	Stato
_____	_____	_____	_____	_____	_____

Il registro è riservato e soggetto a controllo degli accessi.

ALLEGATO E

DICHIARAZIONE DI RISERVATEZZA E NON DIVULGAZIONE

Il soggetto autorizzato ad accedere ai fascicoli SAP-CIAP dichiara:

1. di utilizzare le informazioni esclusivamente per le finalità istituzionali autorizzate;
2. di non divulgare dati personali o documenti riservati senza valida autorizzazione;
3. di rispettare le misure di sicurezza adottate;
4. di segnalare immediatamente eventuali violazioni o accessi non autorizzati;
5. di non utilizzare le informazioni per finalità politiche, economiche o personali;
6. di rispettare gli obblighi di riservatezza anche dopo la cessazione dell'incarico, nei limiti previsti dalla legge.

Nome e cognome: _____

Incarico: _____

Data e firma: _____

ALLEGATO F

MATRICE DELLE RESPONSABILITÀ OPERATIVE

Funzione	Responsabilità principale
Organo competente C.I.A.P.	Approvazione e indirizzo istituzionale
Responsabile SAP-CIAP	Coordinamento generale
Unità ricezione	Acquisizione delle segnalazioni
Unità rischio	Valutazione e classificazione
Unità documentale	Custodia e integrità dei fascicoli
Unità raccordo	Comunicazioni istituzionali
Unità monitoraggio	Aggiornamento dei casi
Revisore indipendente	Controllo procedurale

ALLEGATO G

STANDARD MINIMI DI OPERATIVITÀ DEL SAP-CIAP

Prima dell'attivazione effettiva del sistema devono essere predisposti:

1. nomina formale del Responsabile SAP-CIAP;
2. individuazione dei soggetti autorizzati;
3. canale sicuro di ricezione delle segnalazioni;
4. registro riservato;
5. procedura di classificazione del rischio;
6. informativa sul trattamento dei dati personali;
7. procedura di gestione degli incidenti informatici;
8. procedura di reclamo e riesame;
9. protocollo per le comunicazioni urgenti;
10. disponibilità di personale competente;
11. risorse tecniche e finanziarie adeguate;
12. verifica preliminare della conformità normativa.

L'attivazione è subordinata alla verifica documentata della sussistenza di tali condizioni.

DISPOSIZIONE FINALE DI ADOZIONE

Il presente **Protocollo internazionale n. 04/2026 per la protezione preventiva dei popoli, dei testimoni, dei rappresentanti, dei difensori dei diritti e dei segnalanti** è predisposto quale strumento istituzionale della C.I.A.P. – Corte Internazionale per l'Autodeterminazione dei Popoli, nell'ambito del progetto ordinamentale S.I.P.S.E.

La sua approvazione, applicazione e attuazione sono rimesse agli organi competenti secondo le fonti istitutive e le procedure interne formalmente adottate.

La C.I.A.P. promuove una cultura istituzionale nella quale la protezione della persona precede la formalizzazione del conflitto, la documentazione precede il giudizio e la giustizia costituisce il fondamento della pace.

Venezia – Palazzo Ducale | Ginevra
11 novembre 2026

Per la C.I.A.P. – Corte Internazionale per l'Autodeterminazione dei Popoli

Il Presidente / Organo competente

Il Responsabile istituzionale

Il Segretario della Cancelleria

C.I.A.P. – S.I.P.S.E.

PAX NON ABSENTIA BELLI SED PRAESENTIA IUSTITIAE

Fine del Protocollo n. 04/2026 – Versione 1.0