SIPSE – COMMISSIONE DI CERTIFICAZIONE, CONFORMITÀ E GIUSTIZIA

ATTO N. 18/CCJC

Regolamento generale dell'identità digitale, dell'autenticazione, della gestione delle credenziali, delle autorizzazioni e della sicurezza informatica del Sistema SIPSE-CCJC

Codice: SIPSE-CCJC-ATTO-18 · Versione 1.0 · Testo per approvazione

PREAMBOLO

La Commissione di Certificazione, Conformità e Giustizia del Sistema delle Istituzioni dei Popoli per la Sovranità Economica (SIPSE-CCJC),

- considerata la necessità di assicurare che ogni soggetto autorizzato a operare nelle infrastrutture digitali SIPSE sia identificabile, autenticato e associato a specifiche responsabilità;
- riconosciuta l'esigenza di garantire riservatezza, integrità, disponibilità, tracciabilità e sicurezza delle informazioni e dei servizi digitali;
- ritenuto necessario disciplinare in modo uniforme il ciclo di vita delle identità digitali, delle credenziali, delle autorizzazioni e degli accessi;
- richiamati, quali riferimenti tecnici e metodologici, i principi di gestione del rischio, sicurezza delle informazioni, controllo degli accessi e continuità operativa presenti negli standard internazionali pertinenti;
- tenuto conto, ove applicabili, del Regolamento (UE) 2016/679, del quadro europeo in materia di identificazione elettronica e servizi fiduciari, della normativa nazionale applicabile e delle disposizioni in materia di sicurezza informatica;
- in coordinamento con l'Atto n. 13/CCJC, relativo al codice etico e deontologico, con l'Atto n. 15/CCJC, relativo ai reclami e ai ricorsi interni, con l'Atto n. 16/CCJC, relativo al controllo interno e alla gestione del rischio, e con l'Atto n. 17/CCJC, relativo alla gestione documentale e alla conservazione digitale;

adotta il seguente Regolamento.

Principio fondamentale: nessuna operazione digitale rilevante all'interno del sistema SIPSE-CCJC deve essere eseguita attraverso identità anonime, credenziali condivise o autorizzazioni prive di una base organizzativa documentata, salvo le eccezioni tecniche strettamente necessarie e sottoposte a controlli compensativi.

PARTE I – DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente Regolamento disciplina:
a. l'identificazione e la registrazione delle identità digitali;
b. i processi di verifica dell'identità;
c. l'autenticazione degli utenti e dei sistemi;
d. il rilascio, l'utilizzo, la protezione e la revoca delle credenziali;
e. l'attribuzione e la gestione delle autorizzazioni;
f. la sicurezza degli accessi alle piattaforme SIPSE-CCJC;
g. la gestione delle identità tecniche e dei servizi automatizzati;
h. il monitoraggio degli accessi e degli eventi di sicurezza;
i. la gestione delle compromissioni e degli incidenti relativi alle identità digitali;
j. la disattivazione e la cancellazione controllata degli account.

2. Il Regolamento stabilisce requisiti organizzativi, procedurali e tecnici minimi per la gestione sicura delle identità digitali.

Articolo 2 – Finalità

1. Le finalità sono:
a. assicurare l'attribuibilità delle operazioni ai soggetti autorizzati;
b. impedire accessi non autorizzati;
c. ridurre il rischio di furto, abuso o compromissione delle credenziali;
d. proteggere i registri, gli atti e le infrastrutture digitali;
e. assicurare la separazione delle responsabilità;
f. rendere verificabili le operazioni amministrative e tecniche;
g. garantire la continuità dei servizi;
h. tutelare i diritti degli utenti e degli organismi coinvolti.

Articolo 3 – Ambito di applicazione

1. Il Regolamento si applica agli organi, agli uffici, agli organismi, ai collaboratori e ai soggetti esterni che accedono, in forza di un titolo autorizzativo, alle infrastrutture digitali SIPSE-CCJC.
2. Si applica alle piattaforme, ai registri, ai sistemi documentali, ai portali, alle interfacce applicative, agli ambienti di verifica e alle infrastrutture di comunicazione gestite o utilizzate dal sistema.
3. Si applica anche agli account tecnici, alle identità di servizio e ai dispositivi che effettuano operazioni automatizzate.
4. L'accesso di soggetti esterni è regolato da apposita autorizzazione e, ove necessario, da accordi contrattuali o convenzionali.

Articolo 4 – Natura e limiti del sistema di identità

1. Il sistema di identità digitale SIPSE-CCJC costituisce un'infrastruttura organizzativa interna, destinata all'identificazione degli utenti e alla gestione degli accessi ai servizi del sistema.
2. La registrazione di un'identità nel sistema non equivale automaticamente al rilascio di un'identità digitale riconosciuta da un'autorità pubblica.
3. Le credenziali SIPSE-CCJC non costituiscono, per il solo fatto del loro rilascio, identità elettroniche qualificate, firme elettroniche qualificate, certificati qualificati o strumenti di identificazione aventi efficacia pubblicistica.

4. L'eventuale utilizzo di strumenti riconosciuti dalla normativa vigente deve avvenire nel rispetto dei relativi requisiti e attraverso prestatori o soggetti legittimati.

Articolo 5 – Definizioni

Ai fini del presente Regolamento si intende per:

1. **Identità digitale SIPSE:** insieme dei dati identificativi e degli attributi associati a un soggetto registrato nel sistema.
2. **Identificativo univoco:** codice interno assegnato a ciascuna identità.
3. **Autenticazione:** processo mediante il quale viene verificata la legittimità dell'accesso di un soggetto o sistema.
4. **Credenziale:** elemento utilizzato per autenticare un'identità.
5. **Autorizzazione:** concessione documentata di uno o più permessi operativi.
6. **MFA:** autenticazione a più fattori.
7. **RBAC:** controllo degli accessi basato sui ruoli.
8. **ABAC:** controllo degli accessi basato su attributi e condizioni.
9. **Account privilegiato:** account dotato di poteri amministrativi o tecnici elevati.
10. **Identità di servizio:** identità assegnata a un'applicazione, a un processo automatico o a un servizio informatico.
11. **Revoca:** cessazione dell'efficacia di una credenziale o autorizzazione.
12. **Sospensione:** interruzione temporanea dell'operatività di un'identità o di un accesso.
13. **Evento di sicurezza:** attività o circostanza che può compromettere identità, credenziali, accessi o infrastrutture.
14. **Accesso di emergenza:** accesso straordinario sottoposto a controlli specifici e successivo riesame.

Articolo 6 – Principi generali

1. La gestione delle identità digitali si fonda sui principi di:
a. identificazione individuale;
b. unicità dell'account personale;
c. privilegio minimo;
d. necessità di conoscere;
e. separazione dei compiti;
f. proporzionalità dei controlli;
g. tracciabilità;
h. responsabilità individuale;
i. sicurezza fin dalla progettazione;
j. protezione dei dati personali;
k. verificabilità indipendente.

2. Ogni autorizzazione deve essere limitata alla funzione per la quale è stata concessa.
3. Ogni accesso deve essere revocabile e sottoposto a verifica periodica.

Articolo 7 – Coordinamento con gli altri atti SIPSE-CCJC

1. Il presente Regolamento integra:
   a. l'Atto n. 13/CCJC, per gli obblighi etici e deontologici;

b. l'Atto n. 15/CCJC, per contestazioni, reclami e ricorsi;
c. l'Atto n. 16/CCJC, per controllo interno, rischio e incidenti;
d. l'Atto n. 17/CCJC, per documentazione, integrità e conservazione.

2. In caso di conflitto tra disposizioni, prevalgono le norme imperative applicabili e gli atti di rango superiore del sistema, secondo la rispettiva competenza.
3. Le procedure tecniche devono essere coerenti con il presente Regolamento e documentate.

Articolo 8 – Divieto di abuso

1. È vietato:
   a. utilizzare identità altrui;
   b. condividere credenziali personali;
   c. aggirare i controlli di autenticazione;
   d. concedere accessi non autorizzati;
   e. alterare o cancellare registrazioni di sicurezza;
   f. utilizzare privilegi per finalità estranee;
   g. creare account non autorizzati;
   h. mantenere attivi accessi dopo la cessazione del relativo titolo.
2. Le violazioni sono sottoposte alle procedure di verifica previste dagli atti SIPSE-CCJC, nel rispetto del contraddittorio e delle garanzie applicabili.

PARTE II – MODELLO DI IDENTITÀ DIGITALE E CICLO DI VITA

Articolo 9 – Soggetti titolari di identità digitale

1. Possono essere registrati:
a. organi istituzionali SIPSE;
b. componenti degli organi CCJC;
c. responsabili di ufficio;
d. auditor e ispettori;
e. valutatori e certificatori;
f. esperti tecnici;
g. operatori amministrativi;
h. rappresentanti di organizzazioni aderenti;
i. utenti autorizzati;
j. fornitori e soggetti esterni;
k. applicazioni e servizi informatici.

2. Le identità personali e quelle tecniche devono essere mantenute distinte.

Articolo 10 – Identificativo univoco

1. A ciascun soggetto registrato è assegnato un identificativo univoco interno.
2. L'identificativo:
   a. non deve essere riutilizzato per un altro soggetto;
   b. deve consentire la correlazione con il relativo fascicolo;

c. deve rimanere stabile per il periodo di conservazione previsto;
d. non deve contenere dati personali eccedenti o non necessari.

3. L'identificativo non costituisce di per sé prova dell'identità civile del titolare.

Articolo 11 – Attributi dell'identità

1. L'identità può comprendere, nei limiti della necessità:
   a. identificativo interno;
   b. nome o denominazione;
   c. tipologia del soggetto;
   d. organismo di appartenenza;
   e. funzione o ruolo;
   f. stato dell'identità;
   g. livello di verifica;
   h. data di attivazione;
   i. data di scadenza o revisione;
   j. riferimenti all'autorizzazione;
   k. recapito istituzionale.
2. I dati raccolti devono essere pertinenti, esatti e limitati alle finalità dichiarate.

Articolo 12 – Verifica dell'identità

1. Prima dell'attivazione di un'identità personale deve essere svolta una verifica proporzionata al rischio dell'accesso richiesto.
2. La verifica può basarsi su:
   a. documentazione identificativa;
   b. attestazione dell'organismo di appartenenza;
   c. verifica attraverso canali istituzionali;
   d. strumenti di identificazione elettronica disponibili;
   e. verifica diretta da parte di un responsabile autorizzato.
3. La verifica deve essere documentata senza conservare copie integrali di documenti quando non siano necessarie.
4. I dati di verifica devono essere protetti da accessi non autorizzati.

Articolo 13 – Livelli interni di verifica

1. Il sistema adotta i seguenti livelli organizzativi:
   a. **Livello V1 – Identità dichiarata:** identità registrata sulla base di dati dichiarati, senza verifica documentale completa;
   b. **Livello V2 – Identità verificata:** identità verificata mediante documentazione o attestazione attendibile;
   c. **Livello V3 – Identità rafforzata:** identità verificata con controlli ulteriori, proporzionati alla sensibilità delle funzioni.
2. I livelli sono classificazioni interne e non equivalgono automaticamente ai livelli di garanzia previsti da normative o schemi pubblici.
3. Le funzioni di maggiore impatto richiedono almeno il livello V2 e, ove giustificato dal rischio, V3.

Articolo 14 – Richiesta di registrazione

1. La richiesta di registrazione deve indicare:
   a. soggetto richiedente;
   b. funzione richiesta;
   c. organismo di appartenenza;
   d. servizi ai quali si richiede accesso;
   e. durata prevista;
   f. responsabile proponente;
   g. eventuali esigenze di accesso privilegiato.
2. La richiesta è presentata attraverso il modulo dell'Allegato A.
3. La richiesta non produce automaticamente il diritto all'attivazione.

Articolo 15 – Approvazione dell'identità

1. L'identità è approvata dal responsabile competente per la funzione richiesta.
2. Le identità con privilegi amministrativi richiedono una doppia approvazione.
3. Il soggetto che approva non può coincidere, quando ciò comprometta la separazione dei compiti, con il solo soggetto richiedente.
4. Ogni approvazione deve essere registrata.

Articolo 16 – Attivazione

1. L'attivazione avviene dopo:
   a. verifica dell'identità;
   b. approvazione della richiesta;
   c. assegnazione del ruolo;
   d. consegna sicura delle credenziali;
   e. presa visione delle regole d'uso;
   f. completamento dell'autenticazione prevista.
2. L'attivazione deve essere registrata nel Registro delle Identità Digitali.
3. Le credenziali iniziali devono essere temporanee o soggette a completamento sicuro della procedura di attivazione.

Articolo 17 – Rinnovo e revisione

1. Le identità devono essere sottoposte a revisione almeno annuale.
2. Per account privilegiati e funzioni critiche la revisione deve essere almeno semestrale.
3. La revisione verifica:
   a. permanenza del rapporto o titolo;
   b. necessità dell'accesso;
   c. correttezza dei ruoli;
   d. adeguatezza dei privilegi;
   e. eventuali anomalie.
4. La mancata conferma può comportare sospensione cautelativa dell'accesso.

Articolo 18 – Sospensione

1. L'identità può essere sospesa:
   a. in caso di sospetta compromissione;
   b. in presenza di anomalie rilevanti;

c. durante verifiche di sicurezza;
d. in caso di cessazione temporanea delle funzioni;
e. in presenza di richiesta motivata dell'organismo competente.

2. La sospensione deve essere proporzionata, motivata e registrata.
3. Quando possibile, il titolare deve essere informato, salvo esigenze investigative o di sicurezza.

Articolo 19 – Revoca e disattivazione

1. L'identità deve essere revocata o disattivata:
   a. alla cessazione definitiva della funzione;
   b. alla conclusione del rapporto autorizzativo;
   c. in caso di perdita dei requisiti;
   d. in caso di compromissione non sanabile;
   e. per decisione motivata dell'autorità interna competente.
2. La revoca comporta la disabilitazione degli accessi e delle credenziali correlate.
3. La conservazione delle registrazioni storiche segue l'Atto n. 17/CCJC e la normativa applicabile.
4. La revoca dell'accesso non comporta automaticamente la cancellazione dei documenti o degli atti già prodotti dal soggetto.

Articolo 20 – Identità non trasferibile

1. L'identità personale è individuale e non trasferibile.
2. È vietato consentire ad altri soggetti di operare utilizzando il proprio account.
3. In caso di sostituzione temporanea, deve essere rilasciata una distinta autorizzazione al sostituto.
4. Ogni operazione deve essere attribuibile all'identità effettivamente utilizzata.

Articolo 21 – Account temporanei

1. Gli account temporanei possono essere rilasciati per attività circoscritte.
2. Devono avere:
   a. motivazione;
   b. responsabile;
   c. ambito di accesso;
   d. data di scadenza;
   e. modalità di revoca automatica o verificata.
3. È vietato utilizzare account temporanei per eludere i controlli ordinari.

Articolo 22 – Identità di soggetti cessati

1. Alla cessazione del rapporto, l'identità è disabilitata senza ritardo ingiustificato.
2. Gli accessi attivi, le sessioni e i token devono essere revocati.
3. Eventuali attività di passaggio di consegne devono essere effettuate mediante account distinti e autorizzati.
4. La storia operativa è conservata nei limiti previsti dalle regole di conservazione.

PARTE III – AUTENTICAZIONE E GESTIONE DELLE SESSIONI

Articolo 23 – Obbligo di autenticazione

1. L'accesso alle risorse non pubbliche SIPSE-CCJC richiede autenticazione.
2. L'autenticazione deve essere adeguata alla sensibilità del servizio e al rischio dell'operazione.
3. L'accesso pubblico in sola lettura può essere consentito senza autenticazione, purché non esponga dati riservati o funzioni operative.

Articolo 24 – Fattori di autenticazione

1. Possono essere utilizzati:
   a. fattori di conoscenza;
   b. fattori di possesso;
   c. fattori di inerenza, ove appropriati e proporzionati.
2. La combinazione di fattori deve essere progettata in modo da ridurre il rischio di compromissione.
3. Il sistema privilegia, ove tecnicamente possibile, metodi resistenti al phishing, quali passkey e chiavi di sicurezza hardware.

Articolo 25 – Autenticazione a più fattori

1. L'MFA è obbligatoria per:
   a. amministratori di sistema;
   b. responsabili della sicurezza;
   c. operatori dei registri riservati;
   d. responsabili della gestione documentale e della conservazione;
   e. auditor e certificatori con accesso a fascicoli riservati;
   f. utenti che effettuano operazioni ad alto impatto.
2. L'MFA è raccomandata per tutti gli utenti autenticati.
3. Per le funzioni critiche devono essere preferiti fattori resistenti al phishing.
4. L'eventuale impossibilità tecnica deve essere motivata e compensata da misure alternative.

Articolo 26 – Password e segreti di autenticazione

1. Le password, ove utilizzate, devono essere:
   a. individuali;
   b. non riutilizzate tra servizi critici;
   c. conservate mediante algoritmi di derivazione adeguati e parametri aggiornati;
   d. mai memorizzate in chiaro;
   e. protette da tentativi automatizzati di accesso.
2. Devono essere consentite password robuste e non artificialmente limitate da regole prive di giustificazione tecnica.
3. Il cambio periodico obbligatorio non è richiesto in assenza di un rischio specifico; la modifica è invece necessaria in caso di compromissione sospetta o accertata.

4. Il sistema deve impedire, per quanto tecnicamente possibile, l'utilizzo di password note come compromesse o manifestamente deboli.

Articolo 27 – Protezione contro gli accessi automatizzati

1. Le piattaforme devono adottare misure contro:
   a. tentativi ripetuti di accesso;
   b. credential stuffing;
   c. password spraying;
   d. automazioni abusive;
   e. tentativi di enumerazione degli account.
2. Le misure devono evitare blocchi sproporzionati e consentire procedure sicure di recupero.
3. Gli eventi sospetti devono essere registrati e valutati.

Articolo 28 – Autenticazione rafforzata per operazioni sensibili

1. Può essere richiesta una nuova autenticazione prima di:
   a. modificare autorizzazioni;
   b. esportare archivi riservati;
   c. approvare certificazioni;
   d. modificare o revocare identità;
   e. accedere a funzioni amministrative;
   f. compiere operazioni irreversibili.
2. Le operazioni sensibili devono essere sottoposte a conferma esplicita.
3. Quando opportuno, è richiesta una seconda approvazione indipendente.

Articolo 29 – Gestione delle sessioni

1. Le sessioni devono essere protette contro furto, riutilizzo e fissazione.
2. Devono essere previsti:
   a. scadenza per inattività;
   b. durata massima;
   c. invalidazione dopo disconnessione;
   d. revoca delle sessioni compromesse;
   e. protezione dei token.
3. Le sessioni privilegiate devono avere durata più breve rispetto alle sessioni ordinarie.
4. I parametri tecnici sono definiti nella baseline di sicurezza.

Articolo 30 – Dispositivi attendibili

1. L'accesso a funzioni critiche può essere limitato a dispositivi gestiti o conformi ai requisiti minimi di sicurezza.
2. I dispositivi utilizzati per attività riservate devono essere protetti da:
   a. aggiornamenti di sicurezza;
   b. blocco automatico;
   c. cifratura, ove disponibile;
   d. protezione antimalware o controlli equivalenti;

e. separazione degli account;
f. procedure di cancellazione o revoca in caso di perdita.

3. L'utilizzo di dispositivi personali è subordinato a una valutazione del rischio e a regole specifiche.

Articolo 31 – Recupero dell'accesso

1. Il recupero di un account deve prevedere una verifica adeguata dell'identità.
2. Non è consentito ripristinare un account sulla sola base di una richiesta proveniente dallo stesso canale compromesso.
3. Il recupero deve essere registrato.
4. In caso di account privilegiati è richiesta una verifica rafforzata e una seconda approvazione.

Articolo 32 – Account di emergenza

1. Possono essere predisposti account di emergenza per garantire la continuità dei servizi.
2. Gli account devono essere:
   a. limitati nel numero;
   b. custoditi con procedure sicure;
   c. utilizzati solo in circostanze eccezionali;
   d. sottoposti a registrazione rafforzata;
   e. verificati dopo ogni utilizzo.
3. Ogni utilizzo deve essere comunicato all'Unità di Controllo Interno.
4. È vietato utilizzare gli account di emergenza per attività ordinarie.

Articolo 33 – Identità macchina e autenticazione dei servizi

1. Ogni servizio automatizzato che accede a risorse SIPSE-CCJC deve disporre di un'identità tecnica distinta.
2. Sono vietate credenziali tecniche condivise tra servizi diversi, salvo eccezioni documentate e temporanee.
3. Le comunicazioni tra sistemi devono utilizzare protocolli sicuri e meccanismi di autenticazione adeguati.
4. Le chiavi e i segreti delle applicazioni devono essere gestiti attraverso strumenti protetti, non incorporati in codice sorgente pubblico o distribuito.

PARTE IV – GESTIONE DELLE CREDENZIALI E DELLE CHIAVI

Articolo 34 – Rilascio delle credenziali

1. Le credenziali sono rilasciate esclusivamente dopo l'approvazione dell'identità e dell'autorizzazione.
2. Il rilascio deve avvenire attraverso canali protetti e verificabili.
3. Le credenziali iniziali non devono essere trasmesse in chiaro attraverso canali non sicuri.
4. La consegna deve essere registrata senza conservare il segreto stesso nel registro amministrativo.

Articolo 35 – Custodia delle credenziali

1. Ogni titolare è responsabile della custodia delle proprie credenziali.
2. È vietato:
   a. annotare segreti in luoghi accessibili a terzi;
   b. trasmetterli tramite messaggi non protetti;
   c. conservarli in documenti non cifrati;
   d. condividerli con colleghi o collaboratori;
   e. inserirli in sistemi o applicazioni non autorizzati.
3. Per gli account privilegiati è richiesto l'uso di strumenti di custodia sicura delle credenziali, ove disponibili.

Articolo 36 – Gestione centralizzata dei segreti

1. Le credenziali tecniche, le chiavi applicative e i segreti di servizio devono essere conservati in sistemi dedicati di gestione dei segreti, ove tecnicamente possibile.
2. L'accesso ai sistemi di custodia deve essere limitato e registrato.
3. I segreti non devono essere inclusi nei log, nei report o nei documenti di assistenza.
4. L'accesso amministrativo al sistema di custodia deve essere separato dall'accesso ordinario alle applicazioni.

Articolo 37 – Rotazione delle credenziali

1. Le credenziali tecniche devono essere ruotate secondo una politica basata sul rischio, sulla durata e sulle caratteristiche del sistema.
2. La rotazione è obbligatoria in caso di:
   a. compromissione;
   b. cessazione di un amministratore che ne conosca il contenuto;
   c. esposizione accidentale;
   d. modifica sostanziale dell'architettura;
   e. richiesta motivata del responsabile della sicurezza.
3. Le credenziali personali non devono essere cambiate arbitrariamente con frequenza tale da incentivare pratiche insicure.

Articolo 38 – Chiavi crittografiche

1. Le chiavi crittografiche devono essere generate, conservate, utilizzate e revocate secondo procedure documentate.
2. Le chiavi utilizzate per funzioni diverse devono essere separate, ove tecnicamente possibile.
3. Le chiavi private non devono essere divulgate né inserite in registri amministrativi.
4. Le operazioni critiche di generazione, esportazione e revoca devono essere soggette a controlli rafforzati.
5. L'eventuale impiego di moduli hardware di sicurezza deve essere valutato in base al rischio e alla criticità del servizio.

Articolo 39 – Certificati digitali e infrastrutture PKI

1. I certificati digitali possono essere utilizzati per autenticazione, cifratura, firma o identificazione dei servizi.
2. Il loro impiego deve essere coerente con lo scopo tecnico e con le condizioni di rilascio.
3. Il sistema SIPSE-CCJC non attribuisce autonomamente a un certificato la qualifica giuridica prevista dalla normativa.
4. La qualificazione di firme, sigilli, certificati o servizi fiduciari dipende esclusivamente dal rispetto dei requisiti normativi e dall'intervento dei soggetti legittimati.

Articolo 40 – Smarrimento o furto

1. Il titolare deve segnalare immediatamente lo smarrimento, il furto o la sospetta compromissione di un dispositivo o di una credenziale.
2. Il responsabile competente deve valutare senza ritardo:
   a. sospensione dell'identità;
   b. revoca dei token;
   c. invalidazione delle sessioni;
   d. sostituzione delle credenziali;
   e. verifica degli accessi effettuati.
3. L'evento deve essere registrato nel Registro degli Eventi di Sicurezza.

Articolo 41 – Revoca delle credenziali

1. La revoca deve essere eseguita in caso di cessazione, compromissione o perdita del titolo autorizzativo.
2. La revoca deve interessare tutte le credenziali correlate, incluse quelle tecniche e le sessioni persistenti.
3. Deve essere verificata l'effettiva disabilitazione.
4. La revoca è documentata con data, motivazione, soggetto esecutore e verifica conclusiva.

Articolo 42 – Credenziali di fornitori e soggetti esterni

1. Le credenziali di soggetti esterni devono essere individuali e limitate alle attività autorizzate.
2. Devono essere soggette a scadenza e riesame.
3. Non è ammesso l'accesso permanente di un fornitore senza una motivazione documentata.
4. La cessazione del rapporto comporta la revoca degli accessi.

PARTE V – AUTORIZZAZIONI E CONTROLLO DEGLI ACCESSI

Articolo 43 – Principio di autorizzazione preventiva

1. L'autenticazione dimostra, secondo il livello adottato, il controllo di una credenziale associata a un'identità.
2. L'autenticazione non attribuisce automaticamente il diritto di accedere a tutte le risorse.
3. Ogni accesso deve essere autorizzato in base alla funzione, alla necessità e al rischio.

Articolo 44 – Modello RBAC

1. Il sistema adotta come modello ordinario il controllo degli accessi basato sui ruoli.
2. A ciascun ruolo corrispondono permessi predeterminati e documentati.
3. I ruoli devono essere definiti in modo da evitare privilegi eccessivi.
4. Le assegnazioni devono essere registrate e periodicamente riesaminate.

Articolo 45 – Modello ABAC

1. Per servizi complessi o ad elevata sensibilità può essere adottato un controllo basato su attributi.
2. Le condizioni possono riguardare:
   a. organismo di appartenenza;
   b. funzione ricoperta;
   c. tipologia di documento;
   d. stato del procedimento;
   e. livello di riservatezza;
   f. durata dell'autorizzazione;
   g. contesto dell'accesso;
   h. dispositivo utilizzato.
3. Le regole ABAC devono essere documentate, verificabili e sottoposte a test.

Articolo 46 – Privilegio minimo

1. Ogni utente deve disporre soltanto dei permessi strettamente necessari.
2. I permessi devono essere circoscritti per funzione, risorsa e durata.
3. Le autorizzazioni generiche o illimitate sono vietate, salvo necessità tecniche motivate e controllate.

Articolo 47 – Separazione dei compiti

1. Le funzioni incompatibili devono essere separate.
2. In particolare, ove possibile, devono essere distinti:
   a. richiedente e approvatore dell'accesso;
   b. amministratore tecnico e responsabile del controllo;
   c. auditor e soggetto sottoposto ad audit;
   d. valutatore e decisore finale della certificazione;
   e. operatore del registro e soggetto che autorizza modifiche critiche.
3. Quando la dimensione organizzativa non consente una separazione completa, devono essere previste misure compensative e verifiche indipendenti.

Articolo 48 – Profili di ruolo

1. Sono istituiti, a titolo organizzativo, i seguenti profili:
   a. **Amministratore di sistema:** gestione tecnica dell'infrastruttura;
   b. **Responsabile della sicurezza:** definizione e verifica delle misure di sicurezza;
   c. **Responsabile Gestione Documentale (RGD):** gestione dei flussi documentali;
   d. **Responsabile della Conservazione (RCon):** funzioni previste dall'Atto n. 17/CCJC;

e. **Unità di Controllo Interno (UCI):** verifiche e controlli;
f. **Auditor:** accesso ai fascicoli e alle evidenze pertinenti all'incarico;
g. **Valutatore:** esame tecnico secondo il mandato;
h. **Certificatore:** accesso alle funzioni decisionali attribuite;
i. **Responsabile del Registro:** gestione delle registrazioni autorizzate;
j. **Operatore amministrativo:** gestione delle attività di supporto;
k. **Utente istituzionale:** accesso alle risorse assegnate;
l. **Utente esterno:** accesso circoscritto a uno specifico servizio o procedimento;
m. **Identità tecnica:** accesso applicativo automatizzato.

2. I profili possono essere ulteriormente articolati in sotto-ruoli.
3. Nessun profilo attribuisce competenze istituzionali diverse da quelle formalmente conferite.

Articolo 49 – Autorizzazioni straordinarie

1. Le autorizzazioni straordinarie sono concesse per esigenze specifiche e motivate.
2. Devono indicare:
   a. finalità;
   b. risorse interessate;
   c. permessi concessi;
   d. durata;
   e. soggetto autorizzante;
   f. controlli compensativi.
3. Alla scadenza, l'autorizzazione deve cessare automaticamente o essere revocata mediante procedura verificata.

Articolo 50 – Elevazione temporanea dei privilegi

1. L'elevazione dei privilegi è consentita soltanto per attività determinate.
2. Deve essere limitata nel tempo.
3. Ogni elevazione deve essere registrata.
4. Le attività compiute con privilegi elevati sono sottoposte a riesame.
5. È vietato mantenere privilegi amministrativi permanenti quando sia disponibile una modalità temporanea più sicura.

Articolo 51 – Revisione degli accessi

1. Le autorizzazioni sono riesaminate almeno annualmente.
2. Gli accessi privilegiati sono riesaminati almeno ogni sei mesi.
3. La revisione deve verificare la permanenza della necessità, la correttezza del ruolo e l'assenza di privilegi incompatibili.
4. Gli esiti sono registrati nel Registro delle Autorizzazioni.

Articolo 52 – Accessi ai documenti riservati

1. L'accesso ai documenti riservati è subordinato alla funzione e alla necessità di conoscenza.
2. L'accesso deve essere limitato al fascicolo o alla porzione documentale pertinente.
3. Le esportazioni e le copie devono essere tracciate secondo le regole dell'Atto n. 17/CCJC.
4. L'accesso a un documento non attribuisce il diritto di modificarlo, divulgarlo o utilizzarlo per finalità estranee.

Articolo 53 – Accessi di emergenza

1. L'accesso di emergenza è ammesso esclusivamente per ripristinare servizi o prevenire un danno rilevante.
2. Deve essere autorizzato, ove possibile, da due soggetti indipendenti.
3. In caso di urgenza non differibile, il responsabile tecnico può intervenire, motivando l'azione e informando tempestivamente l'organo di controllo.
4. Ogni utilizzo è sottoposto a riesame successivo.

PARTE VI – SICUREZZA DELL'ARCHITETTURA E DELLE INFRASTRUTTURE

Articolo 54 – Sicurezza fin dalla progettazione

1. Le piattaforme SIPSE-CCJC devono essere progettate secondo criteri di sicurezza fin dalla progettazione e per impostazione predefinita.
2. La sicurezza deve essere considerata nelle fasi di analisi, sviluppo, acquisizione, configurazione, esercizio e dismissione.
3. Le modifiche rilevanti devono essere sottoposte a valutazione del rischio.

Articolo 55 – Segmentazione delle infrastrutture

1. Le infrastrutture devono essere organizzate in ambienti distinti, ove tecnicamente possibile:
   a. produzione;
   b. collaudo;
   c. sviluppo;
   d. amministrazione;
   e. conservazione;
   f. backup e ripristino.
2. L'accesso tra ambienti deve essere controllato.
3. I dati reali non devono essere utilizzati in ambienti di test se non adeguatamente protetti e, ove possibile, anonimizzati o pseudonimizzati.

Articolo 56 – Cifratura delle comunicazioni

1. Le comunicazioni contenenti credenziali, dati personali o informazioni riservate devono utilizzare protocolli di trasmissione sicuri e aggiornati.
2. I protocolli obsoleti o notoriamente vulnerabili devono essere disabilitati.
3. Le configurazioni crittografiche devono essere riesaminate periodicamente.

Articolo 57 – Cifratura dei dati conservati

1. I dati sensibili o riservati devono essere protetti mediante misure di cifratura proporzionate al rischio.

2. Le chiavi devono essere custodite separatamente dai dati cifrati, ove tecnicamente possibile.
3. L'accesso alle chiavi deve essere ristretto e registrato.

Articolo 58 – Configurazioni sicure

1. I sistemi devono essere configurati secondo baseline di sicurezza documentate.
2. Devono essere disabilitati servizi, porte, account e funzionalità non necessari.
3. Le configurazioni critiche devono essere sottoposte a controllo delle modifiche.
4. Le eccezioni devono essere motivate, approvate e riesaminate.

Articolo 59 – Aggiornamenti e vulnerabilità

1. Il sistema deve disporre di una procedura di gestione delle vulnerabilità.
2. Le vulnerabilità devono essere classificate in base a gravità, esposizione e impatto.
3. Gli aggiornamenti di sicurezza devono essere applicati con priorità proporzionata al rischio.
4. Le vulnerabilità critiche esposte a sfruttamento attivo devono essere trattate con urgenza.
5. Le eccezioni temporanee devono prevedere misure compensative e una data di risoluzione.

Articolo 60 – Protezione degli endpoint

1. I dispositivi utilizzati per accedere ai sistemi riservati devono essere protetti contro malware e accessi non autorizzati.
2. Devono essere adottati aggiornamenti, controlli di integrità, blocco automatico e gestione sicura degli utenti.
3. I dispositivi compromessi devono essere isolati o esclusi dall'accesso fino alla verifica.

Articolo 61 – Sicurezza delle applicazioni

1. Le applicazioni devono essere sottoposte a verifiche di sicurezza prima della messa in esercizio.
2. Devono essere valutati almeno:
   a. autenticazione;
   b. autorizzazione;
   c. gestione delle sessioni;
   d. validazione degli input;
   e. protezione delle API;
   f. gestione degli errori;
   g. esposizione dei dati;
   h. dipendenze software.
3. Le vulnerabilità rilevate devono essere registrate e gestite.

Articolo 62 – Sicurezza delle API

1. Le interfacce applicative devono essere protette mediante autenticazione e autorizzazione.
2. Ogni API deve avere uno scopo, un titolare e un ambito di accesso documentati.
3. Devono essere applicati limiti di utilizzo e controlli contro abusi e accessi automatizzati.
4. Le chiavi API devono essere individualizzate per applicazione o servizio, ove possibile.
5. Le API non più necessarie devono essere disattivate.

Articolo 63 – Backup e ripristino

1. Le informazioni e le configurazioni critiche devono essere sottoposte a backup.
2. I backup devono essere protetti da accessi non autorizzati e da alterazioni.
3. Devono essere effettuate prove periodiche di ripristino.
4. Le procedure devono definire obiettivi di ripristino coerenti con la criticità del servizio.
5. La gestione dei backup deve essere coordinata con l'Atto n. 16/CCJC e l'Atto n. 17/CCJC.

Articolo 64 – Fornitori tecnologici

1. I fornitori che trattano o accedono a risorse SIPSE-CCJC devono essere sottoposti a valutazione proporzionata al rischio.
2. Devono essere definiti:
   a. perimetro dell'accesso;
   b. obblighi di riservatezza;
   c. requisiti di sicurezza;
   d. gestione degli incidenti;
   e. restituzione o cancellazione dei dati;
   f. modalità di cessazione del rapporto.
3. Ove applicabile, devono essere formalizzati i ruoli e gli obblighi previsti dalla normativa sulla protezione dei dati personali.
4. L'affidamento a terzi non elimina la responsabilità di supervisione dell'organismo SIPSE competente.

Articolo 65 – Riferimenti tecnici

1. Le procedure tecniche possono utilizzare come modelli di riferimento:
   a. ISO/IEC 27001 e ISO/IEC 27002;
   b. ISO/IEC 27005;
   c. ISO/IEC 27017 e ISO/IEC 27018, ove pertinenti;
   d. NIST Cybersecurity Framework;
   e. linee guida tecniche di organismi riconosciuti.
2. Il richiamo a uno standard non costituisce attestazione di conformità o certificazione.
3. L'eventuale dichiarazione di conformità deve essere sostenuta da valutazioni, evidenze e verifiche effettive.

PARTE VII – REGISTRAZIONE, MONITORAGGIO E RILEVAZIONE

Articolo 66 – Registrazione degli eventi

1. Il sistema deve registrare gli eventi rilevanti per la sicurezza delle identità e degli accessi.
2. Sono registrati, almeno:
   a. accessi riusciti e falliti;
   b. attivazioni e disattivazioni;
   c. modifiche dei ruoli;
   d. assegnazioni e revoche dei privilegi;

e. utilizzo degli account di emergenza;
f. accessi amministrativi;
g. esportazioni di dati riservati;
h. modifiche delle configurazioni critiche;
i. eventi di compromissione;
j. operazioni sui registri delle identità.

Articolo 67 – Contenuto dei log

1. I log devono contenere, ove pertinente:
   a. identificativo dell'identità;
   b. data e ora;
   c. risorsa interessata;
   d. tipo di operazione;
   e. esito;
   f. identificativo tecnico della sessione;
   g. informazioni tecniche strettamente necessarie.
2. Non devono contenere password, token, chiavi private o altri segreti.
3. La raccolta deve rispettare i principi di minimizzazione e proporzionalità.

Articolo 68 – Integrità dei log

1. I log devono essere protetti da alterazioni e cancellazioni non autorizzate.
2. Devono essere adottati controlli di accesso e misure di integrità.
3. Per gli eventi critici possono essere impiegati meccanismi di firma, concatenazione crittografica o archiviazione non modificabile.
4. Tali meccanismi costituiscono misure tecniche di integrità e non attribuiscono automaticamente valore probatorio privilegiato o efficacia pubblicistica alle registrazioni.

Articolo 69 – Monitoraggio

1. Il monitoraggio deve rilevare comportamenti anomali e tentativi di abuso.
2. Possono essere analizzati:
   a. frequenza degli accessi;
   b. tentativi falliti;
   c. accessi fuori dai normali schemi operativi;
   d. modifiche anomale dei privilegi;
   e. esportazioni inconsuete;
   f. accessi da dispositivi non riconosciuti.
3. Il monitoraggio deve essere proporzionato e non può trasformarsi in sorveglianza indiscriminata degli utenti.

Articolo 70 – Allarmi di sicurezza

1. Gli eventi ad alto rischio devono generare allarmi indirizzati ai responsabili competenti.
2. Gli allarmi devono essere classificati secondo gravità e urgenza.
3. Il sistema deve consentire la registrazione della presa in carico, dell'analisi e della risoluzione.

Articolo 71 – Accesso ai log

1. L'accesso ai log è riservato ai soggetti autorizzati.
2. Gli amministratori non devono poter modificare unilateralmente le registrazioni delle proprie attività privilegiate.
3. Le verifiche sui log devono essere documentate.
4. L'accesso da parte dell'UCI deve essere garantito nei limiti del mandato e delle regole di riservatezza.

Articolo 72 – Conservazione delle registrazioni

1. I tempi di conservazione sono stabiliti in una politica documentata, in relazione alla finalità, al rischio e agli obblighi applicabili.
2. Non è prevista una conservazione illimitata generalizzata.
3. Le registrazioni necessarie per un incidente, un reclamo o un procedimento interno possono essere preservate secondo una procedura di conservazione mirata.
4. La conservazione deve essere coordinata con l'Atto n. 17/CCJC.

PARTE VIII – INCIDENTI RELATIVI A IDENTITÀ E ACCESSI

Articolo 73 – Definizione di incidente

1. Costituisce incidente relativo all'identità digitale qualsiasi evento che comprometta o possa compromettere:
   a. un'identità;
   b. una credenziale;
   c. un'autorizzazione;
   d. una sessione;
   e. un dispositivo attendibile;
   f. un servizio di autenticazione;
   g. la riservatezza o integrità dei log.
2. Rientrano nella definizione il furto di credenziali, l'accesso abusivo, l'uso improprio dei privilegi e la creazione non autorizzata di account.

Articolo 74 – Segnalazione

1. Chiunque rilevi un incidente o un sospetto incidente deve segnalarlo senza ritardo al responsabile della sicurezza o al canale designato.
2. La segnalazione deve contenere le informazioni disponibili, senza ritardare la comunicazione per raccogliere dati non essenziali.
3. Il segnalante non deve effettuare autonomamente attività che possano compromettere le evidenze o aggravare l'incidente.

Articolo 75 – Classificazione

1. Gli incidenti sono classificati secondo:
   a. impatto;
   b. estensione;
   c. criticità delle risorse;
   d. sensibilità dei dati;
   e. possibilità di propagazione;
   f. rischio per la continuità operativa.
2. Sono previste almeno quattro classi:
   - **Classe 1 – Bassa:** evento circoscritto senza compromissione accertata;
   - **Classe 2 – Moderata:** anomalia con impatto limitato o rischio concreto;
   - **Classe 3 – Alta:** compromissione significativa o accesso non autorizzato a risorse riservate;
   - **Classe 4 – Critica:** compromissione di account privilegiati, sistemi centrali, registri essenziali o ampia quantità di dati.

Articolo 76 – Contenimento

1. Il responsabile della sicurezza può disporre, secondo necessità:
   a. sospensione dell'identità;
   b. revoca delle credenziali;
   c. invalidazione delle sessioni;
   d. isolamento del dispositivo;
   e. blocco di un'integrazione;
   f. limitazione temporanea del servizio.
2. Le misure devono essere proporzionate e documentate.
3. Il contenimento deve evitare, per quanto possibile, la perdita di evidenze utili.

Articolo 77 – Analisi e ricostruzione

1. L'analisi deve ricostruire:
   a. origine dell'evento;
   b. identità coinvolte;
   c. risorse interessate;
   d. periodo di esposizione;
   e. operazioni effettuate;
   f. eventuali dati coinvolti;
   g. cause tecniche e organizzative.
2. Le evidenze devono essere raccolte e conservate in modo controllato.
3. Le attività di analisi devono essere tracciate.

Articolo 78 – Ripristino

1. Il ripristino avviene dopo la rimozione o il contenimento della causa dell'incidente.
2. Prima della riattivazione devono essere verificate:
   a. sicurezza delle credenziali;
   b. integrità dei sistemi;
   c. correttezza delle autorizzazioni;
   d. assenza di persistenze non autorizzate;
   e. adeguatezza delle misure correttive.

3. La riattivazione di un account privilegiato compromesso richiede approvazione rafforzata.

Articolo 79 – Comunicazioni e notifiche

1. Le comunicazioni interne sono effettuate secondo il livello di gravità.
2. Quando siano coinvolti dati personali, il responsabile competente deve valutare gli obblighi previsti dalla normativa applicabile, compresi gli eventuali obblighi di notifica e comunicazione.
3. Le notifiche alle autorità competenti devono essere effettuate dai soggetti legittimati e nei termini previsti dalla legge.
4. La presente disposizione non introduce termini o obblighi ulteriori rispetto a quelli previsti dalla normativa applicabile.

Articolo 80 – Relazione conclusiva

1. Ogni incidente di Classe 3 o 4 deve essere oggetto di relazione conclusiva.
2. La relazione deve contenere:
   a. descrizione;
   b. cronologia;
   c. impatto;
   d. evidenze;
   e. misure adottate;
   f. cause;
   g. interventi correttivi;
   h. responsabili dell'attuazione;
   i. verifica di efficacia.
3. La relazione è trasmessa all'UCI per le verifiche di competenza.

PARTE IX – IDENTITÀ DI ORGANIZZAZIONI E SOGGETTI TERZI

Articolo 81 – Identità delle organizzazioni

1. Le organizzazioni che accedono alle infrastrutture SIPSE-CCJC possono essere registrate mediante un'identità organizzativa.
2. La registrazione deve indicare:
   a. denominazione;
   b. forma o natura organizzativa dichiarata;
   c. referente autorizzato;
   d. recapiti istituzionali;
   e. titolo di accesso;
   f. servizi richiesti;
   g. durata dell'abilitazione.
3. La registrazione interna non costituisce riconoscimento pubblico della personalità giuridica o della rappresentanza dell'organizzazione.

Articolo 82 – Amministratore dell'organizzazione aderente

1. Ogni organizzazione può designare un referente per la gestione degli accessi dei propri utenti.
2. Il referente:
   a. richiede l'attivazione degli utenti;
   b. comunica variazioni e cessazioni;
   c. verifica la permanenza delle autorizzazioni;
   d. segnala incidenti e anomalie;
   e. assicura la diffusione delle regole interne.
3. Il referente non può attribuire autonomamente privilegi riservati agli organi SIPSE-CCJC.

Articolo 83 – Utenti delegati

1. Gli utenti di un'organizzazione devono essere identificati individualmente.
2. La delega deve indicare le funzioni consentite e la durata.
3. La delega non può essere trasferita senza nuova autorizzazione.
4. Ogni utente delegato risponde delle operazioni compiute attraverso la propria identità, nei limiti delle regole applicabili.

Articolo 84 – Accesso di auditor ed esperti esterni

1. L'accesso di auditor, esperti e valutatori esterni è limitato al mandato ricevuto.
2. Il mandato deve precisare:
   a. oggetto dell'attività;
   b. fascicoli e sistemi consultabili;
   c. durata;
   d. eventuali facoltà di esportazione;
   e. obblighi di riservatezza;
   f. responsabile interno di riferimento.
3. Al termine dell'incarico gli accessi devono essere revocati o rinnovati con nuova autorizzazione.

Articolo 85 – Accessi dei fornitori

1. I fornitori tecnologici accedono alle risorse esclusivamente per le attività contrattualmente o formalmente autorizzate.
2. Gli accessi devono essere individuali, temporanei e monitorati.
3. Le attività privilegiate devono essere autorizzate e, ove possibile, supervisionate.
4. I fornitori non possono creare autonomamente account permanenti o modificare le politiche di accesso.

Articolo 86 – Soggetti non aderenti al SIPSE

1. L'accesso di soggetti non aderenti può essere consentito per:
   a. consultazione di servizi pubblici;
   b. presentazione di istanze;
   c. partecipazione a procedimenti;
   d. consultazione di documenti resi disponibili;
   e. attività di collaborazione autorizzata.
2. Il livello di accesso è determinato in base alla finalità e alla natura del servizio.

3. L'accesso non determina automaticamente adesione al SIPSE né riconoscimento di uno status istituzionale.

Articolo 87 – Accordi di interoperabilità

1. L'interoperabilità con sistemi esterni deve essere disciplinata da un accordo o da un atto tecnico che individui:
   a. soggetti coinvolti;
   b. finalità;
   c. dati scambiati;
   d. modalità di autenticazione;
   e. autorizzazioni;
   f. responsabilità;
   g. sicurezza;
   h. gestione degli incidenti;
   i. cessazione del collegamento.
2. L'interoperabilità non comporta accesso generalizzato ai sistemi interni.
3. Gli scambi devono essere limitati ai dati necessari.

PARTE X – CONDOTTA DEGLI UTENTI E RESPONSABILITÀ

Articolo 88 – Obblighi generali

1. Ogni utente è tenuto a:
   a. utilizzare esclusivamente le proprie credenziali;
   b. proteggere i dispositivi;
   c. rispettare le autorizzazioni;
   d. segnalare anomalie;
   e. non divulgare informazioni riservate;
   f. utilizzare i sistemi per finalità legittime e autorizzate;
   g. collaborare alle verifiche di sicurezza.
2. Gli obblighi si applicano anche agli utenti esterni, nei limiti degli impegni formalmente assunti.

Articolo 89 – Uso accettabile

1. Le risorse digitali devono essere utilizzate esclusivamente per le finalità connesse al servizio o al mandato.
2. È vietato utilizzare le infrastrutture per:
   a. attività illecite;
   b. accessi non autorizzati;
   c. diffusione di malware;
   d. alterazione di registri;
   e. sottrazione di informazioni;
   f. interferenze con la disponibilità dei servizi;
   g. attività estranee che compromettano la sicurezza.

3. Ogni organismo può adottare regole aggiuntive compatibili con il presente Regolamento.

Articolo 90 – Formazione

1. Gli utenti devono ricevere istruzioni adeguate al livello di accesso.
2. Gli utenti privilegiati devono ricevere formazione specifica.
3. La formazione deve comprendere almeno:
   a. protezione delle credenziali;
   b. riconoscimento del phishing;
   c. gestione dei dispositivi;
   d. segnalazione degli incidenti;
   e. trattamento delle informazioni;
   f. uso corretto delle autorizzazioni.
4. La partecipazione può essere documentata nel registro formativo.

Articolo 91 – Phishing e ingegneria sociale

1. Gli utenti devono prestare particolare attenzione a richieste anomale di credenziali, codici, pagamenti o autorizzazioni.
2. Nessun responsabile può richiedere la comunicazione di una password personale.
3. I tentativi di phishing devono essere segnalati attraverso il canale designato.
4. Le simulazioni formative devono essere proporzionate, trasparenti quanto alle regole generali e rispettose della dignità degli utenti.

Articolo 92 – Responsabilità e misure interne

1. La violazione del presente Regolamento può comportare:
   a. richiamo;
   b. formazione correttiva;
   c. limitazione dei privilegi;
   d. sospensione dell'accesso;
   e. revoca dell'abilitazione;
   f. segnalazione all'organo competente.
2. Le misure devono essere proporzionate alla gravità, alla reiterazione e al rischio prodotto.
3. Deve essere garantita la possibilità di conoscere gli addebiti e presentare osservazioni, secondo le procedure applicabili.
4. Restano ferme le responsabilità e le conseguenze previste dalla normativa applicabile.

PARTE XI – CONTROLLO, AUDIT E GARANZIE

Articolo 93 – Funzione di controllo

1. L'UCI esercita le verifiche sul rispetto del presente Regolamento nell'ambito delle competenze attribuite dall'Atto n. 16/CCJC.
2. Le verifiche possono riguardare:
   a. correttezza delle registrazioni;

b. adeguatezza dei privilegi;
c. gestione delle credenziali;
d. revoche e sospensioni;
e. accessi privilegiati;
f. gestione degli incidenti;
g. conformità alle procedure.

3. L'UCI opera con indipendenza funzionale rispetto alle attività sottoposte a controllo.

Articolo 94 – Audit periodici

1. È previsto un programma di audit periodici sulle identità e sugli accessi.
2. Gli audit devono considerare il rischio e la criticità dei servizi.
3. Devono essere verificati almeno:
   a. account inattivi;
   b. account privilegiati;
   c. autorizzazioni scadute;
   d. account condivisi o generici;
   e. accessi di fornitori;
   f. account di emergenza;
   g. eventi anomali;
   h. tempestività delle revoche.
4. Gli esiti sono documentati e trasmessi ai responsabili competenti.

Articolo 95 – Verifiche straordinarie

1. Possono essere disposte verifiche straordinarie in presenza di:
   a. incidente di sicurezza;
   b. sospetto abuso;
   c. segnalazione circostanziata;
   d. modifica sostanziale dell'infrastruttura;
   e. richiesta motivata dell'organo competente.
2. Le verifiche devono rispettare i principi di necessità, proporzionalità e riservatezza.

Articolo 96 – Indipendenza del controllo

1. Il soggetto sottoposto a verifica non può impedire l'accesso alle evidenze pertinenti.
2. Chi ha amministrato direttamente un sistema non può essere l'unico soggetto incaricato di certificare la correttezza delle proprie operazioni.
3. In caso di conflitto di interessi si applicano le regole dell'Atto n. 13/CCJC e dell'Atto n. 16/CCJC.

Articolo 97 – Reclami e contestazioni

1. Gli utenti possono contestare errori di identificazione, sospensioni, revoche o limitazioni degli accessi.
2. Le contestazioni sono trattate secondo l'Atto n. 15/CCJC.
3. La contestazione non determina automaticamente la riattivazione dell'accesso.
4. Le misure cautelative possono essere mantenute quando necessarie a proteggere il sistema, purché siano riesaminate in tempi ragionevoli.

Articolo 98 – Protezione dei segnalanti

1. Le segnalazioni effettuate in buona fede devono essere trattate con riservatezza.
2. È vietata ogni ritorsione interna nei confronti di chi segnali un rischio o un incidente in buona fede.
3. Le segnalazioni manifestamente infondate o effettuate con dolo possono essere valutate secondo le regole applicabili, senza scoraggiare le comunicazioni prudenti di eventi sospetti.

PARTE XII – REGISTRI E DOCUMENTAZIONE

Articolo 99 – Registro delle Identità Digitali (RID)

1. È istituito il Registro delle Identità Digitali SIPSE-CCJC.
2. Il Registro contiene:
   a. identificativo univoco;
   b. tipologia di identità;
   c. dati identificativi strettamente necessari;
   d. livello di verifica;
   e. organismo di appartenenza;
   f. ruolo;
   g. stato dell'identità;
   h. date di attivazione e revisione;
   i. riferimenti alle autorizzazioni.
3. Il Registro non deve contenere password, token, chiavi private o altri segreti di autenticazione.

Articolo 100 – Registro delle Credenziali

1. È istituito il Registro delle Credenziali, limitato ai metadati necessari alla gestione.
2. Può contenere:
   a. identificativo della credenziale;
   b. identità associata;
   c. tipologia;
   d. data di emissione;
   e. data di scadenza;
   f. stato;
   g. data di revoca;
   h. riferimento al sistema di custodia.
3. È vietato registrare il valore segreto della credenziale.

Articolo 101 – Registro delle Autorizzazioni

1. È istituito il Registro delle Autorizzazioni.
2. Contiene:
   a. identità autorizzata;
   b. ruolo;

c. permessi;
d. risorse interessate;
e. responsabile approvatore;
f. motivazione;
g. durata;
h. eventuali limitazioni;
i. esito delle revisioni.

Articolo 102 – Registro degli Eventi di Sicurezza

1. È istituito il Registro degli Eventi di Sicurezza.
2. Il Registro raccoglie gli eventi rilevanti relativi a identità, autenticazione, autorizzazioni e accessi.
3. Deve essere protetto da modifiche non autorizzate.
4. La consultazione è limitata ai soggetti competenti.

Articolo 103 – Registro delle Identità Tecniche

1. È istituito il Registro delle Identità Tecniche e dei Servizi.
2. Per ciascuna identità sono indicati:
   a. denominazione del servizio;
   b. titolare tecnico;
   c. finalità;
   d. risorse accessibili;
   e. privilegi;
   f. sistema di custodia delle credenziali;
   g. data di revisione;
   h. stato.
3. Le identità tecniche prive di titolare responsabile o di finalità documentata devono essere disattivate, previa verifica delle dipendenze operative.

Articolo 104 – Registro delle Revoche

1. È istituito il Registro delle Revoche e delle Disattivazioni.
2. Il Registro documenta:
   a. identità o credenziale interessata;
   b. motivazione;
   c. data e ora;
   d. soggetto che ha disposto la revoca;
   e. soggetto esecutore;
   f. esito della verifica;
   g. eventuali misure successive.
3. Il Registro deve consentire di verificare che la revoca sia stata effettivamente applicata.

Articolo 105 – Responsabilità dei registri

1. La responsabilità organizzativa dei registri è attribuita a un responsabile formalmente designato.
2. Le operazioni di modifica devono essere tracciate.

3. Le attività di amministrazione tecnica non devono consentire alterazioni non rilevabili.
4. La conservazione segue le regole dell'Atto n. 17/CCJC e gli obblighi applicabili.

PARTE XIII – DISPOSIZIONI FINALI E ATTUAZIONE

Articolo 106 – Responsabile della sicurezza delle identità digitali

1. È istituita la funzione di Responsabile della Sicurezza delle Identità Digitali (RSID).
2. Il RSID coordina:
   a. la politica delle identità;
   b. la baseline di autenticazione;
   c. la gestione delle credenziali;
   d. il controllo degli accessi;
   e. la gestione degli incidenti relativi alle identità;
   f. il riesame delle autorizzazioni.
3. Il RSID opera in coordinamento con gli amministratori di sistema, l'UCI e i responsabili documentali.
4. La funzione non attribuisce automaticamente poteri di rappresentanza o competenze istituzionali ulteriori.

Articolo 107 – Politica generale di identità e accesso

1. Entro centoventi giorni dall'entrata in vigore deve essere predisposta la Politica generale di Identità e Accesso (PIA).
2. La PIA deve specificare:
   a. livelli di verifica;
   b. requisiti MFA;
   c. durata delle sessioni;
   d. profili di ruolo;
   e. procedure di recupero;
   f. gestione degli account privilegiati;
   g. revisione degli accessi;
   h. criteri di conservazione dei log.
3. La PIA deve essere riesaminata almeno annualmente.

Articolo 108 – Piano di attuazione

1. L'attuazione avviene secondo il piano di centottanta giorni previsto dall'Allegato J.
2. Le priorità sono:
   a. censimento delle identità;
   b. eliminazione degli account condivisi non giustificati;
   c. attivazione dell'MFA per gli account critici;
   d. revisione dei privilegi;
   e. istituzione dei registri;
   f. definizione delle procedure di revoca;

g. attivazione del monitoraggio;
h. formazione degli utenti.

3. Le attività devono essere documentate e verificate.

Articolo 109 – Riesame del Regolamento

1. Il presente Regolamento è sottoposto a riesame almeno annuale.
2. Il riesame può essere anticipato in caso di:
   a. incidenti rilevanti;
   b. modifiche normative;
   c. cambiamenti tecnologici sostanziali;
   d. nuove esigenze organizzative;
   e. esiti di audit.
3. Le modifiche sono approvate dall'organo competente e registrate secondo l'Atto n. 17/CCJC.

Articolo 110 – Entrata in vigore

1. Il presente Regolamento entra in vigore dalla data della sua approvazione formale.
2. Le strutture interessate sono tenute ad adeguare le proprie procedure secondo il piano di attuazione.
3. Le disposizioni incompatibili con il presente Regolamento sono adeguate o sostituite dagli organi competenti.
4. Restano ferme le disposizioni imperative della normativa applicabile.

ALLEGATI OPERATIVI

Gli allegati costituiscono strumenti applicativi del Regolamento. La loro adozione non sostituisce le verifiche tecniche, organizzative e giuridiche necessarie per l'effettiva operatività delle infrastrutture.

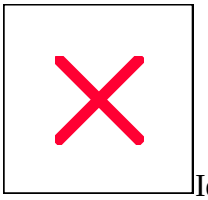
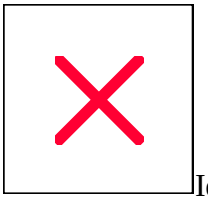
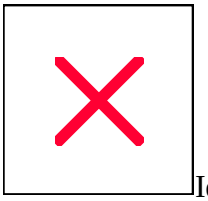
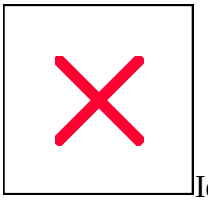
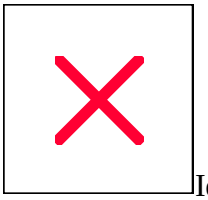
ALLEGATO A – Modulo di registrazione e verifica dell'identità digitale

Codice: SIPSE-CCJC-ATTO-18-A

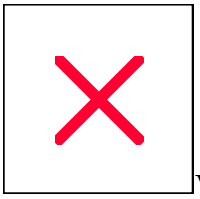
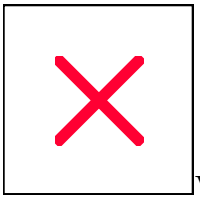
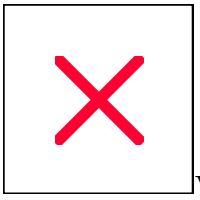
A. Dati del richiedente

- Identificativo interno, se già assegnato:
- Nome e cognome / denominazione:
- Organizzazione di appartenenza:
- Funzione dichiarata:
- Recapito istituzionale:
- Referente responsabile:

B. Identità richiesta

-  Identità personale
-  Identità organizzativa
-  Identità tecnica
-  Identità temporanea
-  Identità di soggetto esterno

C. Verifica

-  V1 – Identità dichiarata
-  V2 – Identità verificata
-  V3 – Identità rafforzata

Modalità di verifica:

- ☒ Documentazione identificativa
- ☒ Attestazione dell'organizzazione
- ☒ Verifica tramite canale istituzionale
- ☒ Identificazione elettronica disponibile
- ☒ Altra modalità documentata

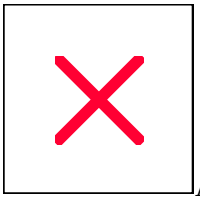
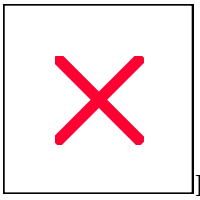
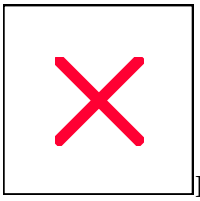
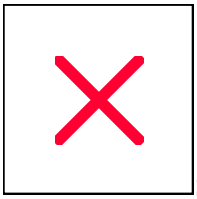
D. Accessi richiesti

- Servizio:
- Ruolo:
- Permessi:
- Motivazione:
- Durata:
- Eventuale accesso privilegiato:

E. Approvazioni

- Responsabile proponente:
- Responsabile approvatore:
- Verifica tecnica:
- Data di attivazione:
- Identificativo assegnato:

F. Esito

-  Approvata
-  Respinta
-  Da integrare
-  Sospesa

ALLEGATO B – Matrice dei ruoli e degli accessi

Profilo	Consultazione	Modifica	Amministrazione	Approvazione
Amministratore di sistema	Sì, per necessità tecnica	Configurazioni	Sì, limitata	No, salvo mandato separato
Responsabile sicurezza	Sì, per controllo	Politiche di sicurezza	Limitata	Secondo competenza
RGD	Documenti pertinenti	Flussi documentali	No, salvo attribuzione	Procedure documentali
RCon	Archivi pertinenti	Metadati e processi autorizzati	No, salvo attribuzione	Procedure di conservazione
UCI	Evidenze di controllo	Rapporti di audit	No	Esiti di controllo
Auditor	Fascicoli assegnati	Evidenze di audit	No	Rapporti di audit
Valutatore	Fascicoli assegnati	Valutazioni	No	Valutazioni tecniche
Certificatore	Fascicoli pertinenti	Atti di competenza	No	Decisioni attribuite
Responsabile Registro	Dati di registro	Registrazioni autorizzate	Limitata	No, salvo attribuzione
Operatore amministrativo	Dati necessari	Attività assegnate	No	No
Utente istituzionale	Risorse autorizzate	Secondo ruolo	No	Secondo mandato

Utente esterno	Risorse autorizzate	Limitata	No	No
Identità tecnica	Risorse di servizio	Operazioni automatizzate	No	No

La matrice è una base generale. Le autorizzazioni effettive devono essere definite per singola piattaforma, risorsa e funzione.

ALLEGATO C – Baseline minima di autenticazione e MFA

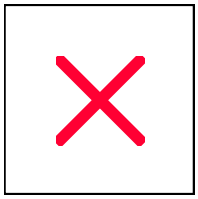
Categoria	Requisito minimo interno
Account amministrativi	MFA obbligatoria, preferibilmente resistente al phishing
Account sicurezza	MFA obbligatoria e accesso ristretto
Account registri riservati	MFA obbligatoria
Auditor e certificatori	MFA obbligatoria per fascicoli riservati
Utenti ordinari	MFA raccomandata; obbligatoria in base al rischio
Utenti esterni	Autenticazione proporzionata alla risorsa
Identità tecniche	Autenticazione macchina-macchina e segreti protetti
Account di emergenza	Custodia rafforzata, utilizzo tracciato e riesame

Ulteriori requisiti:

1. Divieto di credenziali condivise.
2. Blocco o limitazione dei tentativi automatizzati.
3. Recupero dell'accesso mediante verifica indipendente.
4. Revoca tempestiva delle credenziali compromesse.
5. Protezione dei token e delle sessioni.
6. Revisione dei metodi di autenticazione almeno annuale.

ALLEGATO D – Segnalazione di smarrimento, furto o compromissione

Codice: SIPSE-CCJC-ATTO-18-D

- Identità interessata:
- Titolare:
- Data e ora dell'evento:
- Tipo di evento:
  -  Smarrimento dispositivo

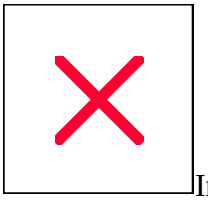
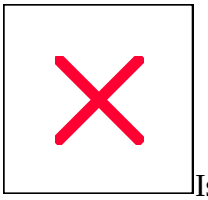
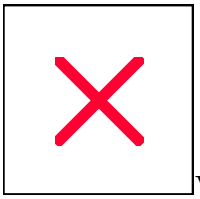
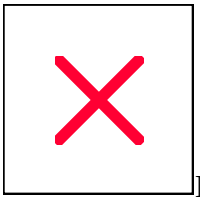
- ☒ Furto dispositivo
- ☒ Password compromessa
- ☒ Token compromesso
- ☒ Sospetto phishing
- ☒ Accesso non riconosciuto
- ☒ Altro

Descrizione dell'accaduto:

Servizi potenzialmente interessati:

Azioni immediate:

- ☒ Sospensione account
- ☒ Revoca credenziali

-  Invalidazione sessioni
-  Isolamento dispositivo
-  Verifica dei log
-  Notifica al responsabile sicurezza

Responsabile della presa in carico:

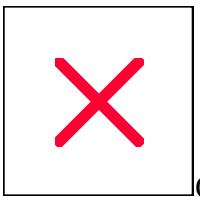
Esito delle verifiche:

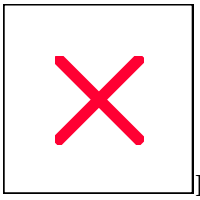
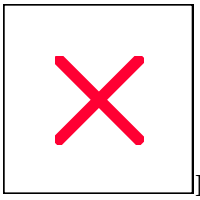
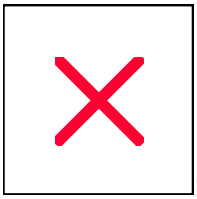
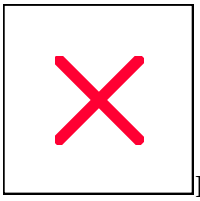
Data di chiusura:

ALLEGATO E – Autorizzazione e revisione periodica degli accessi

Identità:
Organizzazione:
Ruolo assegnato:
Servizi autorizzati:
Permessi concessi:
Motivazione:
Responsabile approvatore:
Data di inizio:
Data di scadenza o revisione:

Esito del riesame:

-  Conferma

-  Riduzione dei privilegi
-  Modifica del ruolo
-  Sospensione
-  Revoca

Motivazione ed evidenze:

Firma o approvazione interna:

ALLEGATO F – Procedura operativa di risposta agli incidenti

Fase 1 – Rilevazione

- Ricezione della segnalazione.
- Registrazione dell'evento.
- Identificazione delle risorse interessate.

Fase 2 – Classificazione

- Valutazione dell'impatto.
- Attribuzione della classe.
- Individuazione del responsabile dell'intervento.

Fase 3 – Contenimento

- Sospensione o revoca degli accessi.
- Isolamento delle risorse compromesse.
- Protezione delle evidenze.

Fase 4 – Analisi

- Ricostruzione cronologica.
- Verifica dei log.
- Individuazione delle cause.

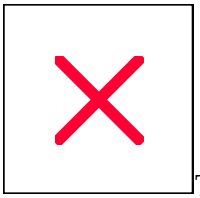
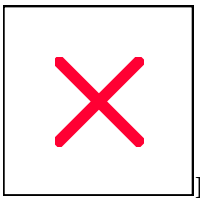
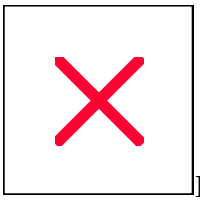
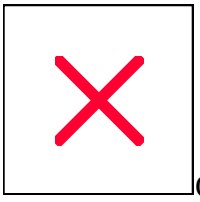
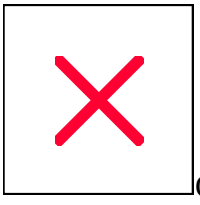
Fase 5 – Ripristino

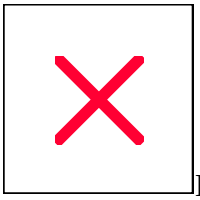
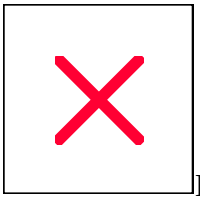
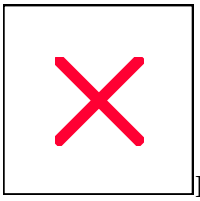
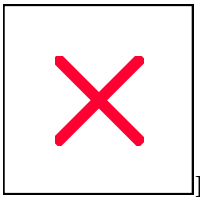
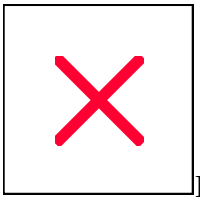
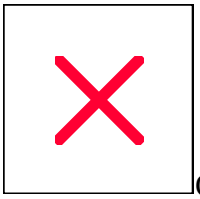
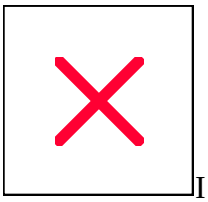
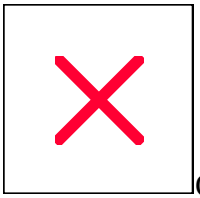
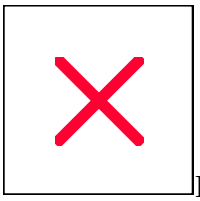
- Rimozione della causa.
- Ripristino sicuro.
- Verifica delle autorizzazioni.
- Riattivazione controllata.

Fase 6 – Chiusura

- Relazione conclusiva.
- Azioni correttive.
- Verifica di efficacia.
- Aggiornamento del registro rischi.

ALLEGATO G – Checklist di audit della sicurezza delle identità

-  Tutte le identità hanno un identificativo univoco.
-  Le identità personali sono individuali.
-  Non risultano account condivisi non giustificati.
-  Gli account inattivi sono riesaminati.
-  Gli account privilegiati sono censiti.

-  L'MFA è attiva per gli account critici.
-  Le credenziali tecniche sono custodite in modo protetto.
-  Le autorizzazioni hanno un responsabile approvatore.
-  Le autorizzazioni scadute sono revocate.
-  Le revoche sono verificate.
-  Gli accessi esterni sono circoscritti.
-  I log sono protetti.
-  Gli account di emergenza sono controllati.
-  Le procedure di recupero sono verificate.

- ☒ Gli incidenti sono registrati e gestiti.
- ☒ Gli utenti hanno ricevuto formazione adeguata.

Esito:

- ☒ Conforme ai requisiti interni verificati
- ☒ Parzialmente conforme
- ☒ Non conforme
- ☒ Non applicabile

Rilievi e azioni correttive:

ALLEGATO H – Accordo per identità e accessi di soggetti terzi

Il soggetto terzo:

- denominazione:
- referente:
- servizio o incarico:
- durata:
- sistemi interessati:

si impegna, nei limiti degli obblighi formalmente assunti, a:

1. utilizzare esclusivamente identità individuali;
2. proteggere le credenziali;
3. rispettare i permessi assegnati;
4. non divulgare informazioni riservate;
5. comunicare tempestivamente gli incidenti;
6. non creare accessi ulteriori senza autorizzazione;
7. restituire o cessare l'utilizzo delle risorse alla fine dell'incarico;
8. collaborare alle verifiche pertinenti.

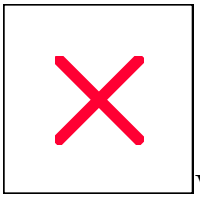
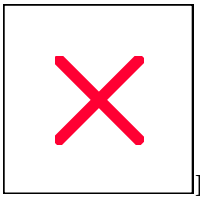
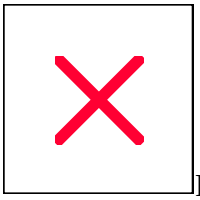
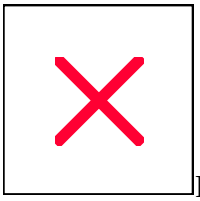
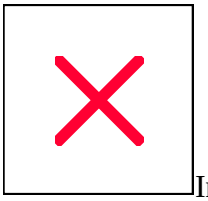
Per il soggetto terzo

Nome, ruolo, data e sottoscrizione.

Per SIPSE-CCJC

Nome, ruolo, data e sottoscrizione.

ALLEGATO I – Checklist di revoca e disattivazione

-  Verifica della cessazione del titolo.
-  Disattivazione dell'account.
-  Revoca delle credenziali.
-  Revoca dei token.
-  Invalidazione delle sessioni.

- ☐ Revoca degli accessi API.
- ☐ Revoca dei certificati o delle chiavi interessate, ove applicabile.
- ☐ Rimozione dai gruppi e dai ruoli.
- ☐ Verifica dell'effettiva disattivazione.
- ☐ Conservazione delle registrazioni necessarie.
- ☐ Aggiornamento dei registri.
- ☐ Comunicazione dell'esito al responsabile competente.

Responsabile esecutore:

Verificatore:

Data e ora:

Esito:

ALLEGATO J – Piano iniziale di attuazione in 180 giorni

Periodo	Attività	Risultato atteso

Giorni 1–30	Censimento di utenti, account e servizi	Inventario iniziale
Giorni 31–45	Classificazione dei livelli di accesso	Matrice dei ruoli
Giorni 46–60	Verifica degli account privilegiati	Elenco privilegi e responsabili
Giorni 61–75	Attivazione MFA per gli account critici	Autenticazione rafforzata
Giorni 76–90	Revisione e revoca degli accessi non necessari	Riduzione della superficie di rischio
Giorni 91–105	Istituzione dei registri	RID e registri complementari
Giorni 106–120	Politica generale di Identità e Accesso	PIA approvata
Giorni 121–135	Monitoraggio e gestione degli incidenti	Procedure e allarmi
Giorni 136–150	Formazione degli utenti	Evidenze formative
Giorni 151–165	Audit iniziale	Rapporto di verifica
Giorni 166–180	Correzioni e validazione	Piano di adeguamento concluso

DISPOSIZIONE DI APPROVAZIONE E ADOZIONE

ATTO N. 18/CCJC

Regolamento generale dell'identità digitale, dell'autenticazione, della gestione delle credenziali, delle autorizzazioni e della sicurezza informatica del Sistema SIPSE-CCJC

Scheda ufficiale dell'atto

Campo	Dato
Codice	SIPSE-CCJC-ATTO-18
Versione	1.0
Stato	Testo predisposto per approvazione
Articoli	110
Allegati	A–J
Ambito	Identità, accessi e sicurezza informatica
Coordinamento	Atti 13, 15, 16 e 17/CCJC
Attuazione	Piano iniziale di 180 giorni

Organo approvante: Commissione di Certificazione, Conformità e Giustizia – SIPSE-CCJC.

Deliberazione di approvazione: n. _____ / CCJC

Data: _____

Luogo: _____

Il Presidente della Commissione

Firma: _____

Il Segretario verbalizzante

Firma: _____

Il Responsabile della Sicurezza delle Identità Digitali

Firma: _____