

Schema di Certificazione ISORS.CERT CIAD ATA

Versione 1 – del 25/02/2026

Sommario

Elementi dello schema

a) Campo di applicazione della certificazione;	4
b) Descrizione del tipo di attività e relativi compiti;	5
b.1) Gestione documentale e archiviazione digitale	5
b.2) Utilizzo di strumenti di produttività	5
b.3) Comunicazione digitale istituzionale	6
b.4) Tutela della sicurezza e della riservatezza dei dati	6
b.5) Supporto alle attività scolastiche e amministrative	6
b.6) Collaborazione in ambienti digitali e di rete	6
c) La competenza richiesta	7
c.1) Alfabetizzazione su informazioni e dati	7
c.2) Comunicazione e collaborazione in ambienti digitali	7
c.3) Creazione di contenuti digitali	7
c.4) Sicurezza digitale	8
c.5) Risoluzione dei problemi e innovazione digitale	8
d) Le capacità	8
d.1) Capacità di utilizzare piattaforme istituzionali	8
d.2) Capacità di organizzare flussi documentali digitali e archiviazione elettronica	9
d.3) Capacità di adottare procedure di cybersecurity per proteggere dati sensibili	9
d.4) Capacità di adattarsi a nuove tecnologie e aggiornare costantemente le proprie competenze	9
e) I prerequisiti	10
e.1) Accesso iniziale (raccomandazioni non vincolanti)	10
e.2) Requisiti per il rinnovo della certificazione	10
e.3) Condizioni aggiuntive	11
e.4) Principio di universalità	11
f) Il codice di condotta	11
f.1) Operare con integrità, imparzialità e trasparenza	11
f.2) Tutelare i dati e la privacy di studenti, colleghi e utenti	12
f.3) Evitare conflitti di interesse nell'utilizzo delle competenze certificate	12
f.4) Promuovere inclusione e accessibilità digitale	12

f.5) Mantenere aggiornate le proprie competenze digitali	12
f.6) Responsabilità e collaborazione professionale	13

Requisiti dello schema

a) Criteri per la certificazione iniziale e per il rinnovo della certificazione.....	14
a.1) Certificazione iniziale	14
a.2) Validità della certificazione	17
a.3) Rinnovo della certificazione	17
b) metodi di valutazione per la certificazione iniziale e per il rinnovo della certificazione	17
b.1) Certificazione iniziale	17
b.2) Rinnovo della certificazione	18
b.3) Principi generali del processo valutativo	19
b.4) Competenze del personale	19
c) metodi e criteri di sorveglianza	20
c.1) Monitoraggio delle piattaforme di esame	Errore. Il segnalibro non è definito.
c.2) Audit interni e verifiche di sistema	Errore. Il segnalibro non è definito.
c.3) Controlli sulle dichiarazioni per il rinnovo	20
c.4) Meccanismi di segnalazione e vigilanza partecipata	20
c.5) Obiettivi della sorveglianza	20
d) criteri per sospendere e revocare la certificazione	21
d.1) Sospensione della certificazione	21
d.2) Revoca della certificazione	21
d.3) Comunicazione del provvedimento	22
d.4) Diritto di ricorso	22
d.5) Obiettivi della sospensione e della revoca	22
e) criteri per modificare il campo di applicazione o il livello della certificazione	23
e.1) Aggiornamenti legati a evoluzioni normative e del framework di riferimento	23
e.2) Introduzione di nuovi livelli o specializzazioni	23
e.3) Revisione periodica dello schema.....	23
e.4) Procedure di comunicazione e trasparenza	24
e.5) Obiettivi delle modifiche	25

SCHEMA DI CERTIFICAZIONE ISORS.CERT CIAD ATA V.1 – 25/02/2026

Elementi dello schema

a) Campo di applicazione della certificazione;

La **Certificazione Internazionale di Alfabetizzazione Digitale – Area ATA (CIAD ATA)** rappresenta uno strumento innovativo di valutazione e riconoscimento delle competenze digitali, concepito specificamente per il personale **Amministrativo, Tecnico e Ausiliario (ATA)** operante nelle istituzioni scolastiche e negli enti formativi, ma estendibile anche a operatori amministrativi e di supporto impiegati presso enti pubblici e privati.

L'obiettivo della certificazione è attestare in maniera oggettiva e standardizzata il possesso delle conoscenze, abilità e competenze digitali necessarie per affrontare in modo efficace le attività quotidiane legate alla gestione amministrativa, alla comunicazione istituzionale e alla sicurezza dei dati, in linea con le più recenti trasformazioni della **pubblica amministrazione digitale** e del mondo del lavoro.

La certificazione si fonda sul **framework europeo DigComp 2.2 (Digital Competence Framework for Citizens)**, adottato dalla Commissione Europea come riferimento per la definizione e la misurazione delle competenze digitali, e copre in maniera integrata le cinque aree di competenza individuate dal modello:

- **Alfabetizzazione su informazioni e dati:** capacità di ricercare, valutare, organizzare e gestire dati, informazioni e contenuti digitali, garantendone l'accuratezza, la pertinenza e l'affidabilità.
- **Comunicazione e collaborazione:** utilizzo consapevole e responsabile delle tecnologie digitali per interagire, comunicare e collaborare in ambienti digitali istituzionali, anche attraverso strumenti di posta elettronica certificata, piattaforme ministeriali e sistemi cloud.
- **Creazione di contenuti digitali:** competenza nella produzione e modifica di documenti, fogli di calcolo, presentazioni multimediali e altri contenuti digitali, rispettando le norme di copyright e le licenze d'uso.
- **Sicurezza:** conoscenze e abilità necessarie a proteggere dispositivi, dati personali e informazioni sensibili, nel rispetto della normativa vigente in materia di **privacy e protezione**

dei dati (GDPR), nonché attenzione agli aspetti di benessere e salute legati all'uso delle tecnologie.

- **Risoluzione dei problemi:** capacità di affrontare e risolvere criticità tecniche nell'uso delle tecnologie digitali, individuando soluzioni efficaci e adattandosi in modo flessibile ai cambiamenti e alle innovazioni tecnologiche.

Lo **schema ISORS.CERT CIAD ATA** non si limita a certificare le abilità di base, ma mira a valorizzare il ruolo strategico del personale ATA e amministrativo come **figura chiave** per il corretto funzionamento delle istituzioni scolastiche e delle strutture organizzative, promuovendo un innalzamento complessivo del livello di competenza digitale e contribuendo a un processo di **modernizzazione e digitalizzazione** delle strutture educative e amministrative.

Il presente schema di certificazione (e successive revisioni) viene reso disponibile tramite pubblicazione nel sito internet www.isors-cert.it.

b) Descrizione del tipo di attività e relativi compiti;

Il personale **ATA certificato ISORS.CERT CIAD ATA** svolge un ruolo essenziale di supporto organizzativo, amministrativo e tecnico nelle istituzioni scolastiche e negli enti formativi, nonché negli enti pubblici e privati che richiedono figure qualificate in grado di operare con strumenti digitali.

La certificazione attesta la capacità del personale di utilizzare in modo efficace, consapevole e sicuro le tecnologie digitali a supporto dei processi gestionali, documentali e comunicativi, garantendo standard di qualità e conformità normativa.

Le attività e i compiti principali possono essere articolati come segue:

b.1) Gestione documentale e archiviazione digitale

- Creazione, gestione, protocollazione e archiviazione di documenti elettronici, nel rispetto delle norme sulla conservazione digitale e sulla trasparenza amministrativa.
- Utilizzo di sistemi di protocollo informatico e di gestione elettronica dei flussi documentali.
- Organizzazione di archivi digitali in modalità sicura e accessibile, anche in cloud.

b.2) Utilizzo di strumenti di produttività

- Redazione di testi amministrativi e comunicazioni istituzionali tramite software di videoscrittura.
- Elaborazione di dati e report mediante fogli di calcolo elettronici.
- Creazione di presentazioni e materiali multimediali a supporto di attività didattiche e amministrative.
- Gestione di moduli e formulari digitali per l'interazione con l'utenza.

b.3) Comunicazione digitale istituzionale

- Gestione di corrispondenza digitale tramite posta elettronica ordinaria e certificata (PEC).
- Utilizzo di piattaforme ministeriali e portali istituzionali (es. SIDI, PagoInRete, registro elettronico).
- Trasmissione e condivisione di atti, circolari e comunicazioni interne ed esterne attraverso sistemi digitali.
- Adozione di un linguaggio chiaro, professionale e conforme alle linee guida della comunicazione pubblica digitale.

b.4) Tutela della sicurezza e della riservatezza dei dati

- Applicazione delle disposizioni normative in materia di protezione dei dati personali (GDPR).
- Utilizzo consapevole di password, credenziali e sistemi di autenticazione.
- Prevenzione di accessi non autorizzati e rischi informatici, attraverso comportamenti corretti e sicuri.
- Adozione di pratiche digitali rispettose del benessere degli utenti e della sicurezza sul lavoro.

b.5) Supporto alle attività scolastiche e amministrative

- Assistenza ai docenti e al personale educativo nell'uso di strumenti informatici e piattaforme di didattica digitale.
- Gestione dei registri digitali, delle presenze e della documentazione legata alla vita scolastica.
- Supporto agli uffici amministrativi nella gestione informatizzata delle pratiche e delle procedure burocratiche.
- Partecipazione all'implementazione di progetti di innovazione e digitalizzazione scolastica.

b.6) Collaborazione in ambienti digitali e di rete

- Utilizzo di piattaforme di condivisione documentale (cloud, drive, repository istituzionali).
- Collaborazione online con colleghi e dirigenti attraverso strumenti di lavoro cooperativo (calendari digitali, task management, videoconferenze).
- Promozione di buone pratiche di team working digitale e di inclusione tecnologica.
- Partecipazione a processi di innovazione organizzativa attraverso l'uso di strumenti digitali collaborativi.

c) La competenza richiesta

Le competenze oggetto della certificazione **ISORS.CERT CIAD ATA** sono definite sulla base del **framework europeo DigComp 2.2 (Digital Competence Framework for Citizens)**, che costituisce il principale riferimento europeo per la misurazione delle competenze digitali. Esse sono articolate nelle cinque aree di competenza e declinate in modo da rispondere alle esigenze operative e organizzative proprie del personale ATA e degli operatori amministrativi.

Le competenze richieste devono consentire al candidato certificato di:

c.1) Alfabetizzazione su informazioni e dati

- Ricercare e reperire informazioni digitali da fonti online istituzionali e affidabili.
- Valutare la qualità, la pertinenza e l'attendibilità delle informazioni digitali, distinguendo tra fonti ufficiali e contenuti non verificati.
- Archiviare e organizzare dati e documenti digitali attraverso strumenti di gestione elettronica e piattaforme cloud, garantendo accessibilità e sicurezza.
- Condividere in modo consapevole file, dati e contenuti digitali, rispettando le procedure e le normative vigenti.

c.2) Comunicazione e collaborazione in ambienti digitali

- Utilizzare strumenti di comunicazione digitale (email, PEC, chat istituzionali, piattaforme collaborative) in maniera chiara, professionale ed efficace.
- Applicare regole di netiquette e comportamenti etici nelle interazioni online.
- Partecipare a gruppi di lavoro e comunità virtuali, contribuendo in modo proattivo a processi di collaborazione e condivisione.
- Utilizzare piattaforme ministeriali e sistemi gestionali digitali in conformità agli standard di sicurezza e riservatezza.

c.3) Creazione di contenuti digitali

- Creare documenti testuali, fogli di calcolo e presentazioni multimediali con strumenti digitali di produttività.
- Integrare e rielaborare contenuti digitali provenienti da fonti diverse, adattandoli ai bisogni istituzionali o organizzativi.
- Applicare correttamente norme e licenze relative al diritto d'autore e al copyright, promuovendo un uso legale delle risorse digitali.
- Sviluppare contenuti accessibili e inclusivi, in grado di rispondere alle esigenze di una utenza diversificata.

c.4) Sicurezza digitale

- Proteggere dispositivi, reti e sistemi da minacce informatiche, adottando comportamenti responsabili e strategie di prevenzione (es. aggiornamenti software, gestione password, uso di antivirus).
- Tutelare la riservatezza dei dati personali e sensibili trattati, nel rispetto del **Regolamento Generale sulla Protezione dei Dati (GDPR)**.
- Promuovere il benessere personale e professionale nell'uso delle tecnologie digitali, prevenendo rischi legati a stress tecnologico o utilizzo improprio dei dispositivi.
- Adottare comportamenti sostenibili, riducendo l'impatto ambientale delle attività digitali (es. gestione dei rifiuti elettronici, risparmio energetico).

c.5) Risoluzione dei problemi e innovazione digitale

- Identificare e risolvere problemi tecnici di base legati all'uso dei dispositivi e delle applicazioni.
- Individuare bisogni organizzativi e proporre soluzioni tecnologiche adeguate e sostenibili.
- Utilizzare le tecnologie digitali in modo creativo, adattando strumenti e metodologie per ottimizzare i processi di lavoro.
- Riconoscere i propri fabbisogni formativi in ambito digitale e intraprendere percorsi di aggiornamento e sviluppo delle competenze.

d) Le capacità

Le capacità operative che il personale certificato **ISORS.CERT CIAD ATA** deve possedere si riferiscono all'applicazione pratica delle competenze digitali, con particolare attenzione al contesto delle istituzioni scolastiche, degli enti formativi e delle strutture amministrative pubbliche e private. Esse riguardano la capacità di utilizzare strumenti, procedure e piattaforme in maniera autonoma, efficace e conforme agli standard normativi.

In particolare, si individuano le seguenti aree di capacità:

d.1) Capacità di utilizzare piattaforme istituzionali

- Gestire in autonomia i principali applicativi ministeriali e scolastici (SIDI, Argo, PagoInRete, registro elettronico, piattaforme INPS e INAIL, portali regionali della formazione e del lavoro).
- Saper navigare tra sezioni e moduli delle piattaforme, compilando e trasmettendo pratiche amministrative e documenti ufficiali.
- Effettuare operazioni di consultazione, inserimento, aggiornamento e stampa di dati in maniera corretta e puntuale.
- Interagire con altre figure professionali (dirigenti, docenti, utenti esterni) attraverso le funzionalità delle piattaforme.

d.2) Capacità di organizzare flussi documentali digitali e archiviazione elettronica

- Definire e gestire procedure per la protocollazione, classificazione e smistamento digitale dei documenti.
- Organizzare archivi digitali strutturati, assicurando la reperibilità e l'accessibilità dei dati da parte degli aventi diritto.
- Applicare procedure di conservazione digitale in conformità alla normativa vigente in materia di amministrazione digitale e trasparenza.
- Ottimizzare i flussi documentali riducendo ridondanze, errori e tempi di gestione.
- Garantire la tracciabilità dei documenti e la corretta archiviazione in cloud o sistemi documentali dedicati.

d.3) Capacità di adottare procedure di cybersecurity per proteggere dati sensibili

- Applicare correttamente politiche di sicurezza informatica (gestione password, sistemi di autenticazione, crittografia dei dati).
- Riconoscere e prevenire rischi informatici, come phishing, malware, accessi non autorizzati o violazioni della privacy.
- Configurare e utilizzare strumenti di protezione (firewall, antivirus, backup automatici).
- Gestire in sicurezza i dati sensibili degli studenti, del personale e degli utenti esterni, nel rispetto delle norme del **GDPR (Reg. UE 2016/679)**.
- Collaborare con i responsabili IT e DPO (Data Protection Officer) per il miglioramento delle politiche di sicurezza informatica.

d.4) Capacità di adattarsi a nuove tecnologie e aggiornare costantemente le proprie competenze

- Dimostrare flessibilità e apertura verso l'adozione di nuove soluzioni digitali introdotte nel contesto scolastico e amministrativo.
- Partecipare a percorsi di formazione continua e autoformazione per aggiornare le proprie conoscenze.
- Individuare e sperimentare nuovi strumenti digitali utili all'ottimizzazione dei processi lavorativi.
- Integrare progressivamente l'uso di applicazioni innovative (cloud collaborativi, piattaforme di e-learning, sistemi di gestione digitale avanzata).
- Promuovere una cultura digitale condivisa all'interno dell'organizzazione, contribuendo alla diffusione di buone pratiche.

e) I prerequisiti

La certificazione **ISORS.CERT CIAD ATA** nasce come strumento di **alfabetizzazione digitale accessibile a tutti**, pertanto **non prevede requisiti minimi vincolanti di accesso**. Ogni candidato, indipendentemente dal titolo di studio posseduto o dall'esperienza lavorativa maturata, può sostenere l'esame e ottenere la certificazione.

Questa impostazione inclusiva risponde a una duplice finalità:

- **Garantire pari opportunità** di accesso alla certificazione a tutto il personale ATA, ma anche ad altri operatori interessati a sviluppare competenze digitali di base e intermedie.
- **Promuovere la diffusione delle competenze digitali** come diritto universale e come prerequisito fondamentale per la cittadinanza attiva e per l'inserimento lavorativo.

Pur non prevedendo barriere di ingresso, lo schema individua alcune **condizioni raccomandate** e criteri orientativi che possono agevolare il candidato nella comprensione dei contenuti d'esame e nell'efficace utilizzo delle competenze certificate.

e.1) Accesso iniziale (raccomandazioni non vincolanti)

- **Conoscenze di base dell'ambiente digitale**: familiarità con l'uso del computer, dei dispositivi mobili e delle principali funzioni di navigazione su Internet.
- **Esperienze pregresse di utilizzo digitale**: minima esperienza, anche informale, nell'impiego di strumenti quali posta elettronica, applicazioni di videoscrittura o ricerca online.
- **Capacità di lettura e comprensione del testo**: livello sufficiente a comprendere istruzioni, quesiti a scelta multipla e contenuti formativi di supporto.

Questi requisiti non sono obbligatori, ma costituiscono **un vantaggio** per affrontare con maggiore serenità le prove di valutazione.

e.2) Requisiti per il rinnovo della certificazione

La certificazione **ISORS.CERT CIAD ATA** ha validità **di 4 anni**. Al termine di tale periodo, per garantire l'attualità delle competenze digitali, il candidato deve dimostrare di aver mantenuto aggiornato il proprio livello di alfabetizzazione.

e.3) Condizioni aggiuntive

- **Disponibilità di strumenti tecnologici per l'esame online:** nei casi in cui il candidato scelga di sostenere la prova a distanza, è necessario disporre di un computer o dispositivo idoneo, con connessione Internet stabile, videocamera e microfono, per consentire il regolare svolgimento delle procedure di **proctoring** e la garanzia di imparzialità della prova.
- **Accessibilità e inclusione:** l'organismo di certificazione garantisce modalità agevolate per candidati con disabilità o bisogni educativi speciali, prevedendo strumenti compensativi o tempi aggiuntivi, nel rispetto della normativa vigente. In caso di disturbi specifici per l'apprendimento (DSA) il sistema prevede 15 minuti aggiuntivi ai tempi previsti per l'esame; in caso di Text to Speech (TTS) il sistema fornisce 30 minuti aggiuntivi ai tempi previsti per l'esame; per tali richieste speciali di assistenza, il richiedente deve fornire un documento giustificativo (es. certificato medico).

e.4) Principio di universalità

Elemento distintivo dello schema ISORS.CERT CIAD ATA è il principio di **universalità dell'accesso**:

- Nessuna esclusione per titolo di studio o livello di competenza pregressa.
- Approccio progressivo che valorizza il candidato a partire dalle sue conoscenze di base.
- Possibilità di utilizzare la certificazione come **primo passo** verso livelli più avanzati di competenza digitale.

f) Il codice di condotta

Il **Codice di condotta** dello schema **ISORS.CERT CIAD ATA** definisce i principi etici, professionali e comportamentali che i candidati certificati devono rispettare nell'esercizio delle proprie mansioni amministrative, tecniche e ausiliarie supportate dall'uso delle tecnologie digitali.

Il rispetto di tali regole garantisce l'integrità della certificazione, la fiducia delle istituzioni scolastiche e formative, la sicurezza degli utenti e la corretta valorizzazione delle competenze acquisite.

f.1) Operare con integrità, imparzialità e trasparenza

- I soggetti certificati ISORS.CERT CIAD ATA devono svolgere tutte le proprie attività digitali e amministrative in modo **onesto, etico e professionale**, evitando comportamenti che possano compromettere la credibilità della certificazione o il corretto funzionamento delle istituzioni.
- Devono applicare le competenze digitali in modo **obiettivo e imparziale**, senza favoritismi verso singoli colleghi, studenti o utenti esterni.
- La **trasparenza** deve essere garantita in ogni fase dei processi amministrativi e documentali, incluse la gestione dei flussi informativi, la protocollazione, la comunicazione istituzionale e la conservazione dei dati.
- **Obiettivo:** assicurare che le decisioni e le attività svolte siano sempre verificabili, tracciabili e coerenti con gli standard di qualità e di legalità.

f.2) Tutelare i dati e la privacy di studenti, colleghi e utenti

- I soggetti certificati devono rispettare rigorosamente la normativa vigente in materia di **protezione dei dati personali**, con particolare riferimento al **Regolamento (UE) 2016/679 – GDPR**.
- È obbligo garantire la **confidenzialità e la riservatezza** delle informazioni trattate, evitando accessi non autorizzati, perdite accidentali o utilizzi impropri.
- Devono essere implementate misure di **sicurezza informatica** nella gestione di piattaforme istituzionali, sistemi informativi scolastici e strumenti di collaborazione digitale.
- **Obiettivo:** assicurare un ambiente digitale sicuro e affidabile, preservando la fiducia di studenti, docenti, colleghi e delle famiglie.

f.3) Evitare conflitti di interesse nell'utilizzo delle competenze certificate

- I soggetti certificati devono operare in modo **imparziale**, evitando che l'uso delle competenze digitali possa generare situazioni di conflitto di interesse.
- Qualsiasi attività di supporto, consulenza o gestione digitale deve essere svolta con **correttezza e obiettività**, senza ricercare vantaggi personali o indebiti benefici.
- Rapporti professionali o economici con fornitori di strumenti digitali devono essere dichiarati e gestiti in conformità con i principi di trasparenza e con le linee guida dello schema.
- **Obiettivo:** garantire che la certificazione sia sempre utilizzata in modo **etico, responsabile e indipendente**.

f.4) Promuovere inclusione e accessibilità digitale

- I soggetti certificati ISORS.CERT CIAD ATA devono favorire pratiche digitali **inclusive**, che rendano l'accesso alle tecnologie e ai servizi equo e non discriminatorio.
- È dovere contribuire alla realizzazione di un ambiente scolastico e amministrativo **accessibile a tutti**, con particolare attenzione a persone con disabilità o bisogni educativi speciali.
- La promozione della cultura digitale deve avvenire in un'ottica di **uguaglianza, cooperazione e sostegno reciproco**, valorizzando diversità e pluralità.
- **Obiettivo:** diffondere buone pratiche di accessibilità e inclusione, a beneficio dell'intera comunità scolastica e istituzionale.

f.5) Mantenere aggiornate le proprie competenze digitali

- I soggetti certificati devono impegnarsi in un **processo di aggiornamento continuo**, partecipando a percorsi di formazione o autoformazione su strumenti digitali e procedure amministrative innovative.
- Si raccomanda ai soggetti certificati di acquisire **flessibilità e adattabilità** nell'utilizzo di nuove tecnologie, applicazioni e piattaforme istituzionali introdotte nelle scuole o negli enti.
- L'aggiornamento può avvenire tramite corsi, workshop, webinar, comunità di pratica o percorsi formativi interni, documentati e riconosciuti.

- **Obiettivo:** garantire che le competenze certificate siano sempre **attuali, pertinenti e coerenti** con l'evoluzione normativa, tecnologica e organizzativa.

f.6) Responsabilità e collaborazione professionale

- Ogni soggetto certificato deve assumersi la **responsabilità diretta** delle attività digitali svolte, operando con attenzione e diligenza.
- Viene suggerito un atteggiamento di **collaborazione costruttiva** con colleghi, dirigenti, docenti e utenti esterni, al fine di migliorare l'organizzazione dei processi digitali.
- Si raccomanda di segnalare tempestivamente eventuali **anomalie, criticità o violazioni** riscontrate nei sistemi informatici o nei flussi di lavoro digitali, contribuendo alla loro risoluzione.
- **Obiettivo:** rafforzare la qualità complessiva dei servizi digitali e la fiducia della comunità scolastica e amministrativa.

Il **Codice di condotta ISORS.CERT CIAD ATA** stabilisce standard chiari in merito a:

- **Integrità, imparzialità e trasparenza** nell'uso delle tecnologie digitali.
- **Tutela della privacy e protezione dei dati** di studenti, colleghi e utenti.
- **Prevenzione dei conflitti di interesse** nell'esercizio delle competenze certificate.
- **Promozione dell'inclusione e dell'accessibilità digitale.**
- **Aggiornamento continuo e responsabilità professionale.**

Requisiti dello schema

a) Criteri per la certificazione iniziale e per il rinnovo della certificazione

L'ottenimento e il rinnovo (facoltativo) della certificazione **ISORS.CERT CIAD ATA** avvengono attraverso procedure chiare e standardizzate, finalizzate ad assicurare l'affidabilità del processo di valutazione e la coerenza con i riferimenti europei in materia di competenze digitali (Framework **DigComp 2.2**).

a.1) Certificazione iniziale

Per conseguire la certificazione ISORS.CERT CIAD ATA, il candidato deve effettuare un esame iniziale strutturato come segue:

- **Tipologia della prova:** test informatizzato a risposta multipla.
- **Numero delle domande:** 168 quesiti, equamente distribuiti sulle 5 aree di competenza DigComp 2.2; le domande vengono proposte per area di competenza partendo dalla prima.

**Griglia di Valutazione Automatica ATA
Certificazione DigCompATA**

Aree di competenza	Domande banche dati	N. domande esame
Area 1 – Informazioni e dati	84	33
1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali	28	10
1.2 Valutare dati, informazioni e contenuti digitali	28	10
1.3 Gestire dati, informazioni e contenuti digitali	28	13
Area 2 – Comunicazione e collaborazione	84	42
2.1 Interagire con gli altri attraverso le tecnologie	14	7
2.2 Condividere informazioni attraverso le tecnologie digitali	14	7
2.3 Esercitare la cittadinanza attraverso le tecnologie digitali	14	7
2.4 Collaborare attraverso le tecnologie digitali	14	7
2.5 Netiquette	14	7
2.6 Gestire l'identità digitale	14	7
Area 3 – Creazione di Contenuti digitali	84	33
3.1 Sviluppare contenuti digitali	21	9
3.2 Integrare e rielaborare contenuti digitali	21	8
3.3 Copyright e licenze	21	8
3.4 Programmazione	21	8
Area 4 – Sicurezza	84	30
4.1 Proteggere i dispositivi	21	8
4.2 Proteggere i dati personali e la privacy	21	8
4.3 Proteggere la salute e il benessere	21	8
4.4 Proteggere l'ambiente	21	6
Area 5 – Risoluzione dei problemi	84	30
5.1 Risolvere problemi tecnici	21	8
5.2 Individuare bisogni e risposte tecnologiche	21	8
5.3 Utilizzare in modo creativo le tecnologie digitali	21	8
5.4 Individuare i divari di competenze	21	6
Totale	420	168

- **Durata della prova:** tempo massimo previsto di 120 minuti.
- **Modalità di svolgimento:**
 1. In presenza presso sedi qualificate dall'organismo di certificazione.
 2. Oppure online con procedure di **proctoring digitale**, per garantire imparzialità e sicurezza.
- **Criteri di valutazione:** punteggio attribuito in base al numero di risposte corrette.
- **Livelli di padronanza** attribuiti in base alla percentuale di risposte corrette:

Dettaglio (1–8)	Livello del Modello	Descrizione delle attività (DigComp 2.2)	Livello ISORS CERT	Range percentuale risposte	Livello numerico certificato
1	Base	Compiti semplici svolti con guida	Base 1	< 25%	1
2	Base	Compiti semplici svolti con crescente autonomia	Base 2	25–49%	2

Dettaglio (1–8)	Livello del Modello	Descrizione delle attività (DigComp 2.2)	Livello ISORS CERT	Range percentuale risposte	Livello numerico certificato
3	Intermedio	Compiti ben definiti e sistematici; problemi diretti	Intermedio 3	50–69%	3
4	Intermedio	Compiti e problemi ben definiti ma non sistematici	Intermedio 4	70–84%	4
5	Avanzato	Compiti e problemi diversi; autonomia elevata	Avanzato 5	85–89%	5
6	Avanzato	Compiti più opportuni in contesti variabili; guida ad altri	Avanzato 6	90–94%	6
7	Altamente specializzato	Risoluzione di problemi complessi con soluzioni limitate	Altamente specializzato 7	95–97%	7
8	Altamente specializzato	Risoluzione di problemi complessi con molti fattori di interazione; progettazione di soluzioni avanzate	Altamente specializzato 8	≥ 98%	8

- **Accessibilità e inclusione:** l’organismo di certificazione garantisce modalità agevolate per candidati con disabilità o bisogni educativi speciali, prevedendo strumenti compensativi o tempi aggiuntivi, nel rispetto della normativa vigente. In caso di disturbi specifici per l’apprendimento (DSA) il sistema prevede 15 minuti aggiuntivi per ogni esame; in caso di Text to Speech (TTS) il sistema fornisce 30 minuti aggiuntivi per ogni esame; per tali richieste speciali di assistenza, il richiedente deve fornire un documento giustificativo (es. certificato medico).
- **Candidati:** Il numero massimo di candidati nella sessione d’esame è 8 totali (sia in presenza che in remoto); le sessioni sono dedicate e possono essere o in presenza o alternativamente in remoto; non sono previste sessioni miste (con candidati sia in presenza che da remoto); qualora la sessione preveda più di 8 candidati, dovrà essere nominato un sorvegliante che avrà il compito di coadiuvare l’esaminatore nella gestione della sessione d’esame.
- **Contenuti del certificato:** Il certificato dovrà riportare almeno i seguenti dati:
 - Ragione sociale dell’OdC, relativo indirizzo ed informazioni di contatto
 - Il marchio dell’OdC e quello di Accredia completo del numero di registrazione dell’accreditamento
 - Nominativo della persona certificata (nome e cognome); non sono ammessi soprannomi o diminutivi
 - Codice fiscale della persona certificata
 - Il numero del certificato
 - Data inizio validità del certificato

- Data di aggiornamento (o modifica) del certificato
- Data di scadenza del certificato
- Riferimento allo schema di certificazione
- Riferimento ai Framework europei sulle competenze digitali (DigComp 2.2)
- Le aree di competenza e per ciascuna area i livelli raggiunti dal candidato
- La firma da parte di personale autorizzato dell'OdC
- Un sistema antifalsificazione

a.2) Validità della certificazione

La certificazione **ISORS.CERT CIAD ATA** ha **validità quadriennale** a partire dalla data di delibera.

Durante il periodo di validità, il certificato resta attivo a condizione che il soggetto certificato rispetti il **Codice di condotta** e non incorra in situazioni che possano comportare sospensione o revoca.

a.3) Rinnovo della certificazione

La certificazione ha una **validità di 4 anni**. Al termine di questo periodo, il soggetto certificato può chiedere di rinnovare il certificato. Il rinnovo della certificazione prevede un esame con le stesse modalità dell'esame per la certificazione iniziale con conseguente rilascio del certificato rinnovato in caso di esito positivo; l'esame e la delibera del rinnovo devono essere effettuate prima della scadenza del certificato per assicurare la continuità nella certificazione.

Il processo di rinnovo garantisce che le competenze certificate:

- Siano **attuali** e coerenti con l'evoluzione delle tecnologie digitali.
- Restino **allineate** alle normative nazionali ed europee in materia di digitalizzazione, sicurezza e protezione dei dati.
- Mantengano un **valore professionale e istituzionale riconosciuto**, a beneficio sia dei soggetti certificati che delle organizzazioni in cui operano.

b) metodi di valutazione per la certificazione iniziale e per il rinnovo della certificazione

Il processo di valutazione adottato nello schema **ISORS.CERT CIAD ATA** è concepito per garantire **oggettività, trasparenza, imparzialità e tracciabilità** dei risultati, nonché per assicurare che la certificazione rappresenti un'effettiva evidenza del possesso delle competenze digitali da parte del candidato.

I metodi di valutazione si articolano in due distinte fasi: **certificazione iniziale** e una seconda fase facoltativa del **rinnovo della certificazione**.

b.1) Certificazione iniziale

- **Tipologia di prova**

- Test informatizzato a risposta multipla (computer-based test – CBT).
- Numero complessivo di domande: 168, equamente distribuite sulle 5 aree di competenza del DigComp 2.2.
- Ogni domanda è composta da 4 opzioni di risposta, di cui una sola corretta.
- **Database dei quesiti**
 - Le domande sono estratte in modo **casuale** da un **database validato**, costantemente aggiornato dall'organismo di certificazione.
 - Il database è strutturato per garantire equilibrio in termini di difficoltà, ambiti tematici e rappresentatività delle competenze.
 - Tutti i quesiti sono validati da un **comitato tecnico** interno
- **Criteri di somministrazione**
 - La prova può svolgersi in presenza, presso sedi qualificate e dotate di postazioni informatiche controllate.
 - In alternativa, l'esame può essere svolto **da remoto**, con sistemi di **proctoring digitale** che consentono il monitoraggio continuo tramite webcam, microfono e tracciamento delle attività del candidato.
 - In entrambi i casi, l'identità del candidato deve essere verificata tramite documento ufficiale valido.
 - Non sono possibili sessioni di esame non presidiate.
- **Attribuzione del punteggio**
 - Ad ogni risposta corretta viene attribuito un punteggio unitario (1 punto).
 - Non è prevista penalizzazione per risposte errate o omesse.
 - Il punteggio finale viene convertito in **percentuale di risposte corrette**, sulla base della quale si determina il livello di padronanza (Base, Intermedio, Avanzato, Altamente specializzato).
 - La mancata risposta è considerata come una risposta errata.
- **Registrazione e tracciabilità**
 - I risultati sono registrati automaticamente dal sistema informatico e archiviati in un database sicuro.
 - Al candidato viene rilasciato un **report individuale** che riporta: punteggio complessivo, livello di competenza raggiunto e dettaglio per area DigComp.
 - Sulla base dei risultati ottenuti, verrà effettuata una proposta di certificazione da parte dell'esaminatore alla commissione di delibera che verificherà il processo di certificazione e delibererà il rilascio del certificato in caso di esito positivo.
 - Pertanto, in caso di esito positivo, al candidato verrà rilasciato un certificato e il suo nome verrà iscritto nell'elenco delle persone certificate che è pubblico e che verrà trasmesso anche all'Ente di Accreditamento.

b.2) Rinnovo della certificazione

Alla scadenza quadriennale della certificazione, il candidato può effettuare il rinnovo della propria certificazione. Il rinnovo della certificazione prevede un esame con conseguente rilascio del certificato rinnovato in caso di esito positivo; l'esame e la delibera del rinnovo devono essere effettuate prima della scadenza del certificato.

b.3) Principi generali del processo valutativo

Indipendentemente dalla modalità scelta, il processo di valutazione per la certificazione iniziale e per il rinnovo deve rispettare i seguenti principi:

- **Imparzialità:** i valutatori non devono trovarsi in situazioni di conflitto di interesse con i candidati.
- **Oggettività:** i risultati sono determinati esclusivamente sulla base delle risposte fornite o delle evidenze documentali, senza margini di discrezionalità.
- **Trasparenza:** al candidato vengono fornite informazioni chiare sulle modalità di valutazione, sui criteri di attribuzione dei punteggi e sugli esiti.
- **Tracciabilità:** ogni prova e ogni documento presentato vengono archiviati e conservati per garantire la possibilità di verifiche successive.
- **Accessibilità:** l'organismo di certificazione garantisce misure compensative e tempi aggiuntivi per candidati con disabilità o bisogni educativi speciali.

b.4) Competenze del personale

Sono definite le competenze del personale che effettua la valutazione:

Esaminatore:

- Diploma Superiore*, preferibile laurea
- Corso interno di 8h per la gestione degli schemi di certificazione*, corsi per formatore, corsi di tecniche informatiche
- Almeno 2 anni di attività lavorativa in ambito della formazione come docente o formatore e/o della certificazione come commissario d'esame*, almeno 1 esame in affiancamento con supervisione personale esperto*
- Conoscenza della norma ISO 17024*, conoscenza del framework DIGCOMP 2.2 e DigCompEdu*

Eventuali esperti:

- Laurea* in materie tecniche, economiche o pedagogiche
- corsi per formatore o docente
- Almeno 5 anni di attività lavorativa in ambito della formazione come formatore e/o della certificazione come commissario d'esame

Comitato di certificazione (organo deliberante):

- Laurea* in materie tecniche, economiche o pedagogiche
- Corso interno di 8h per la gestione degli schemi di certificazione*, corsi per formatore o docente
- Almeno 2 anni di attività lavorativa in ambito della formazione come docente o formatore e/o della certificazione delle competenze come commissario d'esame o responsabile schema*

- Conoscenza della norma ISO 17024, conoscenza del framework DIGICOMP 2.2 e DigCompEdu

Le competenze indicate con * si intendono mandatorie

Sorvegliante:

- conoscenza delle procedure dell'OdC e delle regole di conduzione d'esame.

C) metodi e criteri di sorveglianza

La sorveglianza del sistema di certificazione **ISORS.CERT CIAD ATA**, consente di garantire nel tempo la **validità, l'affidabilità e la credibilità** della certificazione stessa.

Non sono previste delle prove periodiche nell'ambito dei quattro anni di validità della certificazione da parte della persona certificata, ma la persona certificata ha l'obbligo di segnalare all'organismo di certificazione eventuali reclami o provvedimenti (amministrativi/legali) di richiamo o sanzionatori ricevuti che siano relativi al campo di applicazione della certificazione.

c.3) Controlli sulle dichiarazioni per il rinnovo

- **Controlli:** l'organismo di certificazione effettua verifiche sulle pratiche per accertare la veridicità delle attestazioni fornite (es. contatto diretto con i datori di lavoro, verifica presso enti formatori accreditati).
- **Sanzioni:** in caso di dichiarazioni false o non verificabili, il rinnovo della certificazione non viene concesso e il candidato può incorrere nella sospensione o revoca del certificato se ancora in corso di validità.

c.4) Meccanismi di segnalazione e vigilanza partecipata

- **Segnalazioni da parte degli stakeholder:** docenti, dirigenti scolastici, colleghi o utenti esterni possono inoltrare segnalazioni in caso di comportamenti non conformi al Codice di condotta o di sospette irregolarità nell'uso della certificazione.
- **Gestione dei reclami:** l'organismo di certificazione dispone di una procedura formalizzata per la ricezione, la valutazione e la risoluzione dei reclami, garantendo riservatezza e imparzialità.
- **Vigilanza collaborativa:** le segnalazioni e i feedback degli stakeholder costituiscono elemento utile per i processi di sorveglianza e per l'aggiornamento dello schema di certificazione.

c.5) Obiettivi della sorveglianza

L'attività di sorveglianza è finalizzata a:

- **Garantire la qualità** delle procedure di esame e di rinnovo.

- **Assicurare la conformità** ai requisiti normativi, regolamentari e tecnici applicabili.
- **Prevenire comportamenti scorretti** o utilizzi impropri della certificazione.
- **Rafforzare la fiducia** di istituzioni, scuole, enti formativi e utenti finali nella validità della certificazione.
- **Mantenere l'allineamento** dello schema con gli standard europei e internazionali in materia di competenze digitali e processi di certificazione.

c) criteri per sospendere e revocare la certificazione

La sospensione e la revoca della certificazione **ISORS.CERT CIAD ATA** sono misure straordinarie che l'organismo di certificazione può adottare per garantire la **credibilità, l'integrità e la validità** del sistema di certificazione. Tali provvedimenti si applicano nei casi in cui il soggetto certificato non rispetti i requisiti previsti o adotti comportamenti contrari ai principi etici e professionali sanciti dallo schema.

d.1) Sospensione della certificazione

La sospensione comporta l'interruzione temporanea della validità del certificato e l'impossibilità, per il soggetto interessato, di fare uso della certificazione durante il periodo di sospensione. Può essere disposta nei seguenti casi:

- **Inadempienze formali:** irregolarità nella presentazione di documenti o informazioni richieste dall'organismo di certificazione.
- **Segnalazioni durante la validità della certificazione:** accertamento di comportamenti non pienamente conformi al **Codice di condotta**, ma non tali da giustificare immediata revoca.
- **Situazioni temporanee** che possano compromettere la credibilità della certificazione (es. sospensioni disciplinari in ambito lavorativo connesse all'uso improprio delle tecnologie digitali).

Durata della sospensione:

- La sospensione ha durata variabile, ma non superiore a 6 mesi. Decorre dalla data del provvedimento di sospensione.
- Il soggetto interessato deve sanare le cause che hanno determinato il provvedimento entro tale periodo.
- In caso di mancato adeguamento, la sospensione si trasforma automaticamente in **revoca**.

d.2) Revoca della certificazione

La revoca è un provvedimento definitivo che comporta la **decadenza del certificato** e l'impossibilità per il soggetto di continuare a qualificarsi come "Certificato ISORS.CERT CIAD ATA".

La revoca comporta la cancellazione del nominativo della persona certificata da ogni relativo elenco, compreso quello dell'Ente di Accreditamento.

Può essere disposta nei seguenti casi:

- **Violazione grave del Codice di condotta:** utilizzo improprio delle tecnologie digitali, violazioni della normativa sulla protezione dei dati (GDPR), comportamenti non etici o non conformi agli standard professionali.
- **Frode o irregolarità durante l'esame:** utilizzo di mezzi illeciti per superare la prova di certificazione o tentativi di falsificazione dei risultati.
- **Uso improprio della certificazione:** dichiarazioni mendaci sul possesso della certificazione, utilizzo del titolo in contesti estranei allo scopo dello schema o per ottenere vantaggi indebiti.
- **Dichiarazioni false nei rinnovi:** presentazione di documentazione non veritiera o non verificabile a sostegno della richiesta di rinnovo.
- **Comportamenti lesivi dell'immagine dello schema:** azioni che possano danneggiare la reputazione e la credibilità dell'organismo di certificazione o del sistema ISORS.CERT CIAD ATA .

d.3) Comunicazione del provvedimento

Ogni decisione di sospensione o revoca è notificata formalmente al soggetto interessato mediante comunicazione scritta, con indicazione chiara delle motivazioni. La revoca decorre dalla data del provvedimento.

La comunicazione specifica:

- la natura del provvedimento (sospensione o revoca),
- la durata della sospensione o la definitività della revoca,
- le azioni correttive richieste, ove applicabili,
- i termini e le modalità di ricorso.

d.4) Diritto di ricorso

Il candidato ha diritto di presentare **ricorso scritto** entro 30 giorni dalla data del provvedimento o della decisione.

Il ricorso è esaminato da personale che non abbia partecipato all'attività o alla decisione oggetto dell'ricorso stesso che si esprime entro 30 giorni lavorativi dal ricevimento del ricorso.

L'esito del ricorso può confermare, modificare o annullare il provvedimento adottato.

d.5) Obiettivi della sospensione e della revoca

Questi provvedimenti sono finalizzati a:

- Salvaguardare l'**integrità e la credibilità** del sistema di certificazione.
- Assicurare che il titolo "Certificato ISORS.CERT CIAD ATA " mantenga valore e riconoscibilità presso istituzioni, scuole, enti e utenti.

- Prevenire e sanzionare usi impropri, fraudolenti o scorretti della certificazione.
- Promuovere comportamenti conformi ai principi di **etica, trasparenza e responsabilità digitale**.

d) criteri per modificare il campo di applicazione o il livello della certificazione

Il campo di applicazione e i livelli della certificazione **ISORS.CERT CIAD ATA** possono essere modificati per garantire l'allineamento costante dello schema con l'evoluzione normativa, tecnologica e organizzativa, nonché con i fabbisogni formativi ed operativi delle istituzioni scolastiche, degli enti formativi e delle strutture amministrative pubbliche e private.

Le modifiche sono introdotte secondo criteri di **trasparenza, partecipazione e aggiornamento continuo**, e devono essere oggetto di comunicazione ufficiale a tutti i soggetti certificati e agli stakeholder coinvolti.

e.1) Aggiornamenti legati a evoluzioni normative e del framework di riferimento

Framework DigComp: ogni aggiornamento, revisione o nuova versione del quadro europeo delle competenze digitali (DigComp) comporta l'adeguamento dello schema ISORS.CERT CIAD ATA ai nuovi standard.

Normativa nazionale ed europea: l'entrata in vigore di nuove disposizioni in materia di digitalizzazione, amministrazione digitale, protezione dei dati personali, sicurezza informatica e inclusione digitale può determinare modifiche al campo di applicazione della certificazione.

Linee guida ministeriali: eventuali aggiornamenti emanati dal Ministero dell'Istruzione e del Merito (MIM), dal Ministero del Lavoro o da altri enti competenti costituiscono riferimento vincolante per l'adeguamento dello schema.

e.2) Introduzione di nuovi livelli o specializzazioni

- **Nuove tecnologie:** Il campo di applicazione della certificazione può essere aggiornato in risposta a nuove esigenze tecnologiche o metodologiche.
- **Livelli di approfondimento:** oltre ai livelli Base, Intermedio, Avanzato, Altamente specializzato.
- **Certificazioni modulari:** possibilità di suddividere la certificazione in moduli autonomi corrispondenti alle aree DigComp, consentendo ai candidati di certificarsi progressivamente.

e.3) Revisione periodica dello schema

Periodicità: lo schema di certificazione è soggetto a revisione sistematica ogni **3 anni** a meno che non intervengano aggiornamenti normativi previsti al precedente paragrafo e1.

Coinvolgimento degli stakeholder: la revisione avviene attraverso il confronto con:

- comitato tecnico-scientifico,
- rappresentanti delle istituzioni scolastiche,
- associazioni datoriali e professionali,
- enti pubblici e privati utilizzatori della certificazione,
- soggetti già certificati.

Procedura per le modifiche:

- Analisi delle nuove esigenze da parte del **Proprietario dello Schema**.
- Verifica della compatibilità con gli **standard DigComp** e con le linee guida europee.
- Definizione formale del nuovo **campo di applicazione**, con documentazione ufficiale.

Obiettivo: garantire che lo schema resti sempre aggiornato, coerente con i fabbisogni reali del personale docente e formatore e in linea con le best practices internazionali.

e.4) Procedure di comunicazione e trasparenza

Tutte le modifiche al **campo di applicazione** o ai **livelli di competenza** devono essere **formalmente documentate**.

La documentazione deve includere:

- Descrizione dettagliata della modifica.
- Motivazioni e obiettivi dell'aggiornamento.
- Impatto sulla valutazione e sulla certificazione dei candidati.

Comunicazione ufficiale: ogni modifica viene resa pubblica tramite sito web dell'organismo di certificazione, newsletter istituzionali e comunicazioni dirette ai candidati certificati.

Le modifiche devono essere **comunicate ufficialmente** a:

- Tutti i **candidati certificati**, per informarli di eventuali cambiamenti nei requisiti o nei livelli della certificazione.

La comunicazione deve avvenire con **modalità formali**, tramite **piattaforme digitali**, **email ufficiali** o pubblicazione nei documenti ufficiali dello schema.

Chiarezza e anticipo: le modifiche entrano in vigore con congruo anticipo rispetto alle sessioni d'esame, al fine di consentire ai candidati di prepararsi in modo adeguato.

Supporto informativo: vengono messi a disposizione materiali esplicativi, FAQ e linee guida per illustrare in dettaglio le novità introdotte.

e.5) Obiettivi delle modifiche

L'aggiornamento del campo di applicazione o dei livelli della certificazione persegue i seguenti obiettivi:

- **Allineamento** agli standard europei (DigComp) e alle normative nazionali ed internazionali.
- **Rispondenza** alle nuove esigenze operative e tecnologiche del personale docente e formatore.
- **Flessibilità e inclusione**: garantire che la certificazione sia accessibile a diversi profili professionali e che possa evolvere insieme alle competenze richieste.
- **Miglioramento continuo**: rafforzare la credibilità e l'efficacia della certificazione, assicurandone il valore riconosciuto da scuole, enti formativi, pubbliche amministrazioni e mondo del lavoro.

Questo schema definisce in modo chiaro e strutturato le **regole, i criteri e i requisiti** per la certificazione **ISORS.CERT CIAD ATA**, garantendo:

- Trasparenza e standardizzazione del processo di valutazione.
- Allineamento alle migliori pratiche europee e internazionali.
- Riconoscibilità e affidabilità della certificazione.
- Supporto alla **formazione continua** e alla **mobilità professionale** dei soggetti certificati.