Requisiti tecnico-organizzativi per la gestione digitale degli organi collegiali e delle operazioni di voto nelle istituzioni scolastiche

1. Oggetto, finalità e riferimenti normativi

Il presente documento definisce i requisiti tecnico-organizzativi ai fini dell'adozione di soluzioni digitali, da parte delle istituzioni scolastiche, destinate allo svolgimento a distanza alle attività di cui al comma 3, lett. a) e b) dell'articolo 44 del CCNL 2019/2021 che rivestono carattere deliberativo.

Le disposizioni contenute nel presente documento sono finalizzate a garantire, in modo uniforme, la validità giuridica delle deliberazioni, la sicurezza e integrità delle operazioni, nonché la piena conformità alla normativa vigente, con particolare riferimento alla protezione dei dati personali e alla gestione documentale.

Il presente documento è adottato in coerenza con:

- l'art. 44 del CCNL del comparto Istruzione e Ricerca vigente, sottoscritto in data 18 gennaio 2024, che disciplina lo svolgimento a distanza delle attività collegiali deliberative;
- il D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale – CAD);
- il Regolamento (UE) 2016/679 (GDPR);
- il D.Lgs. 196/2003;
- il D.P.R. 275/1999 (autonomia scolastica);
- il D.Lgs. 33/2013 (trasparenza amministrativa);
- le Linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici, sicurezza ICT e identità digitale;
- il DPCM 3 dicembre 2013 e le Linee guida AgID 2020 e successive modifiche.

Ai fini del presente documento, per sistemi di voto online certificati si intendono sistemi che, anche sulla base della documentazione tecnica disponibile, garantiscono il rispetto dei requisiti di sicurezza, integrità, univocità e verificabilità del voto.

Le istituzioni scolastiche, nell'ambito della propria autonomia organizzativa, possono utilizzare strumenti di uso corrente per la gestione delle sedute a distanza e delle votazioni, anche mediante integrazione di più strumenti o procedure organizzative, purché tali soluzioni risultino conformi ai requisiti definiti nel presente documento, sulla base delle funzionalità disponibili e della documentazione tecnica resa disponibile dal fornitore.

2. Principi di base

Le soluzioni adottate devono garantire una serie di principi fondamentali, la cui assenza potrebbe compromettere la validità del processo organizzativo e deliberativo:

- Identificazione e responsabilità: è necessario garantire l'identificazione certa dei partecipanti e la riconducibilità delle azioni agli utenti autenticati. Tale principio può essere derogato esclusivamente nei casi di voto segreto, nei limiti e con le modalità previste dal presente documento.
- Validità giuridica: deve essere assicurata la piena efficacia delle deliberazioni, garantendo la conformità alle disposizioni normative e ai regolamenti d'istituto, nonché la corretta formazione della volontà collegiale.
- Integrità e sicurezza: le soluzioni devono assicurare l'immodificabilità dei dati e dei risultati delle votazioni, nonché la protezione da accessi non autorizzati, alterazioni o perdite di informazioni.
- Trasparenza e verificabilità: deve essere sempre possibile ricostruire e verificare ex post il corretto svolgimento del procedimento deliberativo, attraverso la disponibilità di evidenze documentali e tracciature tecniche.
- Segretezza del voto: nei casi in cui sia previsto il voto a scrutinio segreto, deve essere garantito un anonimato effettivo, non reversibile e tecnicamente dimostrabile, tale da escludere qualsiasi possibilità di correlazione tra identità del votante e voto espresso.

L'eventuale utilizzo di funzionalità di sondaggio o raccolta di opinioni integrate in piattaforme di collaborazione o videoconferenza è ammesso esclusivamente qualora tali funzionalità risultino idonee, per caratteristiche tecniche e modalità d'uso, a soddisfare i requisiti previsti dal presente documento in relazione alla specifica tipologia di votazione.

3. Requisiti di identificazione, autenticazione e accesso

3.1 Identificazione degli utenti

Le soluzioni devono garantire in modo inequivocabile l'identificazione degli utenti, mediante l'utilizzo di identità digitali univoche, non condivise e coerenti con il CAD. Deve essere assicurata la corrispondenza tra identità digitale e soggetto avente diritto alla partecipazione e al voto.

L'identificazione si considera soddisfatta quando il sistema consente di associare in modo univoco ciascun accesso a un soggetto avente diritto e impedisce l'utilizzo condiviso o impersonale delle credenziali.

3.2 Autenticazione

L'accesso ai sistemi deve avvenire tramite meccanismi di autenticazione adeguati al livello di rischio, privilegiando, ove possibile, modalità di autenticazione forte. Devono essere adottate misure idonee a prevenire accessi non autorizzati, utilizzi impropri delle credenziali e fenomeni di impersonificazione.

L’autenticazione si considera adeguata quando il sistema impedisce accessi non autorizzati e consente di tracciare in modo certo l’identità del soggetto che opera.

3.3 Autorizzazioni e gestione dei ruoli

Il sistema deve prevedere una chiara distinzione dei ruoli (ad esempio presidente, segretario, componente) e garantire che ciascun utente possa accedere esclusivamente alle funzionalità strettamente necessarie. Deve essere assicurata la tracciabilità delle operazioni svolte.

3.4 Gestione delle sessioni

Devono essere implementate misure per la gestione sicura delle sessioni, tra cui:

- tracciamento delle sessioni attive;
- interruzione automatica in caso di inattività;
- prevenzione di accessi simultanei non autorizzati.

4. Requisiti delle operazioni di voto

4.1 Requisiti generali

Il sistema di voto deve garantire che ogni avente diritto possa esprimere un solo voto, che il voto sia registrato in modo integro e non modificabile e che l’esito sia determinato in modo corretto e verificabile. Deve essere inoltre assicurato il rispetto dei quorum deliberativi e delle regole procedurali previste.

Nel caso in cui le operazioni di voto siano effettuate mediante strumenti integrati in piattaforme di videoconferenza o collaborazione, deve essere verificato che tali strumenti garantiscano:

- la corretta identificazione dei partecipanti;
- l’univocità dell’espressione di voto;
- la disponibilità di evidenze verificabili dell’esito.

Qualora tali condizioni non siano soddisfatte, gli strumenti possono essere utilizzati esclusivamente per attività non deliberative o per votazioni prive di rilevanza giuridica.

4.2 Voto palese

Nel caso di voto palese, il sistema deve garantire la piena tracciabilità del voto, l’associazione tra votante e scelta espressa e la disponibilità dei risultati ai fini della verbalizzazione e della conservazione.

L’utilizzo di funzionalità di sondaggio integrate in piattaforme di videoconferenza può essere ammesso per il voto palese, purché sia garantita la tracciabilità del voto e la possibilità di

ricondurre in modo certo ciascuna espressione di voto al relativo partecipante, nonché la possibilità di documentare e conservare i risultati.

4.3 Voto a scrutinio segreto

Il voto a scrutinio segreto richiede specifiche garanzie tecniche e organizzative, in quanto incide direttamente sulla libertà e autenticità dell'espressione di voto e sulla validità delle deliberazioni adottate.

L'utilizzo di strumenti di sondaggio o votazione integrati in piattaforme di videoconferenza o collaborazione è ammesso per il voto a scrutinio segreto esclusivamente qualora sia verificato, anche sulla base della documentazione tecnica resa disponibile dal fornitore, che tali strumenti garantiscano effettivamente i requisiti di seguito indicati, in relazione alla tipologia di votazione e al livello di garanzia richiesto.

I requisiti da rispettare sono i seguenti:

- Separazione tra identità e voto: il sistema deve assicurare una separazione strutturale tra la fase di autenticazione e quella di espressione del voto, attraverso meccanismi che impediscano qualsiasi collegamento tra le due.
- Anonimizzazione effettiva: l'anonimato deve essere garantito mediante soluzioni tecniche idonee a impedire in modo definitivo la riconducibilità del voto al votante. Non sono sufficienti soluzioni che dichiarino l'anonimato senza garantirlo tecnicamente.
- Non accessibilità delle informazioni: deve essere esclusa la possibilità che amministratori di sistema, fornitori o altri soggetti possano accedere a informazioni che consentano di risalire al voto individuale.
- Trattamento dei metadati: particolare attenzione deve essere posta ai metadati (quali log e timestamp), che devono essere gestiti in modo tale da non consentire, neanche indirettamente, la re-identificazione del votante.
- Verificabilità dell'esito: il sistema deve consentire la verifica dell'esito complessivo della votazione, senza compromettere in alcun modo la segretezza dei voti individuali.

In particolare, non sono idonee al voto segreto le soluzioni che:

- non garantiscono una separazione effettiva tra identità del votante e voto espresso;
- consentono, anche indirettamente, la riconducibilità del voto al soggetto;
- non permettono di dimostrare tecnicamente l'anonimato delle risposte.

In assenza della verifica dei suddetti requisiti, le soluzioni non sono utilizzabili per votazioni a scrutinio segreto con effetti deliberativi.

5. Sicurezza informatica

Le soluzioni adottate devono essere conformi alle Linee guida AgID in materia di sicurezza ICT e garantire adeguati livelli di protezione.

Devono essere assicurati:

- la cifratura dei dati;
- la protezione da vulnerabilità note e aggiornamenti periodici del sistema;
- il monitoraggio e la registrazione degli accessi;
- la disponibilità di sistemi di audit;
- la segregazione degli ambienti;
- la gestione degli incidenti di sicurezza.

Devono inoltre essere previste misure di continuità operativa, inclusi sistemi di backup e procedure di ripristino.

Nel caso di utilizzo di piattaforme cloud o servizi di terze parti, le istituzioni scolastiche devono verificare:

- la localizzazione dei dati e le modalità di trattamento;
- le misure di sicurezza dichiarate dal fornitore;
- la conformità alle normative europee e nazionali in materia di protezione dei dati.

I requisiti si considerano soddisfatti quando le misure sopra indicate risultano dichiarate dal fornitore o documentate nelle caratteristiche tecniche del sistema utilizzato.

6. Protezione dei dati personali

Il trattamento dei dati deve avvenire nel rispetto dei principi del GDPR, in particolare minimizzazione, limitazione delle finalità, integrità, riservatezza e responsabilizzazione.

Particolare attenzione deve essere posta all'utilizzo di strumenti che prevedono la raccolta di dati tramite servizi esterni o integrati, verificando che:

- i dati trattati siano limitati a quelli strettamente necessari;
- siano chiaramente definiti i ruoli privacy;
- siano disponibili adeguate garanzie contrattuali in relazione al trattamento dei dati.

Di seguito i principali aspetti da tenere in considerazione:

- Nomina del responsabile del trattamento: qualora il servizio sia erogato da un fornitore esterno che tratta dati personali per conto dell'istituzione scolastica, deve essere formalmente nominato responsabile del trattamento ai sensi dell'art. 28 del GDPR.
- Misure di sicurezza: devono essere adottate misure tecniche e organizzative adeguate, tra cui cifratura, pseudonimizzazione o anonimizzazione (ove necessario), controllo degli accessi e sistemi di backup e disaster recovery.

- Valutazione d’impatto: nei casi previsti, e in particolare per i sistemi di voto digitale, deve essere effettuata una valutazione d’impatto sulla protezione dei dati (DPIA).

7. Formazione, gestione e conservazione dei documenti

Le attività devono essere documentate mediante la produzione di verbali digitali, registrazioni degli esiti di voto ed evidenze delle operazioni svolte.

I documenti devono essere immodificabili, completi e associati ai metadati necessari a garantirne autenticità, integrità e contestualizzazione.

La conservazione deve avvenire nel rispetto delle Linee guida AgID, assicurando nel tempo autenticità, integrità, leggibilità e reperibilità dei documenti.

Nel caso di utilizzo di soluzioni che non consentono l’esportazione strutturata dei risultati delle votazioni, deve essere comunque garantita la produzione di evidenze documentali idonee alla verbalizzazione e alla conservazione.

8. Requisiti organizzativi e responsabilità

Le istituzioni scolastiche devono adeguare i regolamenti d’istituto, disciplinando in modo puntuale lo svolgimento delle sedute a distanza e le modalità di voto, con particolare riferimento al voto segreto.

Devono essere individuate, nel rispetto dell’ordinamento scolastico, le figure responsabili della conduzione della seduta e della verbalizzazione, con riferimento alle funzioni tipiche degli organi collegiali (es. Presidente, Segretario verbalizzante).

Devono essere previste procedure per la gestione di eventuali malfunzionamenti, inclusa la sospensione delle operazioni di voto e, se necessario, la loro ripetizione.

9. Verifica di conformità

Le istituzioni scolastiche sono tenute a verificare preventivamente la coerenza delle soluzioni adottate ai requisiti del presente documento, acquisendo idonea documentazione tecnica attestante le caratteristiche del sistema utilizzato, nonché una dichiarazione di conformità da parte del fornitore o partner tecnologico.