



PROTOCOLO DE VOTACIÓN TELEMÁTICA PARA EL COLEGIO OFICIAL DE ENFERMERÍA DE CÓRDOBA.

Procedimiento General. PG-COE Córdoba

Elaborado por: Dpto. Informática	Revisado por: Junta Directiva	Aprobado por: Junta Directiva
Fecha de su aprobación en acta: 16/10/2026 Última Revisión: 16/10/2026	Edición: 04	Área: Secretaría



INDICE DE CONTENIDOS

1. INTRODUCCIÓN	4
1.1. Objeto.....	4
1.2. Ámbito de aplicación	4
1.3. Principios del sistema.....	4
1.4. Definiciones	5
2. ROLES Y RESPONSABILIDADES	6
3. ESQUEMA GENERAL DE FUNCIONAMIENTO	7
4. EVENTOS Y ESCENARIOS DE VOTACIÓN	8
4.1. El evento de votación.....	8
4.2. Modalidades de evento.....	8
4.3. Tipos de votación.....	9
4.4. Opciones de voto.....	9
4.5. Estados de una votación	9
4.6. Votación simultánea presencial y telemática	10
5. CENSO E IDENTIFICACIÓN DEL VOTANTE.....	10
5.1. Censo del evento	10
5.2. Estados del votante	11
5.3. Acceso telemático.....	11
5.4. Acceso presencial	12
5.5. Información a los colegiados.....	12
6. EMISIÓN DEL VOTO TELEMÁTICO.....	12
6.1. Secuencia.....	12
6.2. Qué firma el votante y qué no.....	12
6.3. Comprobaciones antes de admitir un voto	13
6.4. Dónde queda cada dato.....	13
7. VOTO PRESENCIAL Y RECuento EN SALA	14
8. SECRETO DEL VOTO	14
8.1. Separación entre quién vota y qué vota.....	14
8.2. Urna sin orden	15
8.3. Reescritura de la urna al cierre	15
9. CIERRE, SELLADO Y RESULTADOS	16
9.1. Cierre de una votación	16
9.2. Comprobación de integridad	16
9.3. Precinto con OpenTimestamps	16
9.4. Resultados.....	17



10. ACTA DE RESULTADOS.....	17
11. AUDITORÍA Y VERIFICACIÓN.....	18
11.1. Registro de actuaciones	18
11.2. Verificación independiente.....	18
11.3. Qué puede comprobar un auditor.....	18
12. GARANTÍAS DE SEGURIDAD INTERNA	19
12.1. ¿Puede alguien del Colegio saber qué ha votado una persona?	19
12.2. ¿Se pueden añadir votos falsos?	19
12.3. ¿Se puede modificar un voto o un resultado después?	19
12.4. ¿Puede una persona votar dos veces?.....	19
12.5. ¿Se puede votar sin un certificado válido?	19
12.6. Límites que conviene conocer	19
12.7. Reglas operativas	20
13. MARCO LEGAL Y PROTECCIÓN DE DATOS.....	20
13.1. Marco normativo	20
13.2. Firma electrónica y validez	20
13.3. Protección de datos personales.....	21
13.4. Participación de las asesorías	21
14. APROBACIÓN, PUESTA EN MARCHA Y REVISIÓN	21
14.1. Aprobación.....	21
14.2. Prueba piloto.....	21
14.3. Preparación de cada proceso	22
14.4. Revisión del protocolo.....	22
ANEXO I. CRITERIOS DE ACTUACIÓN ANTE INCIDENCIAS	23



1. INTRODUCCIÓN

1.1. Objeto

El presente documento establece el **protocolo de votación telemática** del Colegio Oficial de Enfermería de Córdoba: cómo se organiza un proceso de votación, quién interviene en él, cómo se identifica a cada votante, cómo se emite y se cuenta cada voto y qué garantías ofrece el sistema.

Una vez aprobado por la Junta Directiva, este documento constituye el **reglamento interno de voto telemático** del Colegio y será de aplicación a todas las votaciones que se celebren a través de la plataforma. Ha sido revisado previamente por la asesoría jurídica del Colegio.

El documento describe el funcionamiento del sistema sin entrar en detalles de programación. La documentación técnica completa (arquitectura, código y configuración del servidor) se mantiene por separado y está a disposición de los auditores que la Junta designe.

1.2. Ámbito de aplicación

El protocolo se aplica a las votaciones de los colegiados que la Junta Directiva convoque mediante la plataforma, en cualquiera de estas dos modalidades:

- **Asamblea o sesión en directo**, con votantes en la sala y votantes conectados a distancia al mismo tiempo, retransmisión en vídeo y chat moderado.
- **Consulta telemática de varios días**, solo a distancia, sin retransmisión.

1.3. Principios del sistema

La plataforma se ha diseñado para cumplir seis principios:

Principio	Qué significa en la práctica
Identidad	Solo vota quien está en el censo, y se identifica con su certificado digital de la FNMT o presencialmente con su carné o DNI.
Voto Único	Cada colegiado vota una sola vez en cada votación, sea en la sala o a distancia, nunca de las dos formas.
Secreto del voto	Se sabe quién ha votado, pero no qué ha votado. Una vez cerrada la votación, nadie puede relacionar un voto con su votante, ni siquiera con acceso a la base de datos o a sus ficheros.
Integridad	Los votos no pueden alterarse, añadirse ni eliminarse sin que se detecte.
Verificabilidad	Cualquier auditor puede comprobar, de forma independiente del Colegio, que los resultados corresponden a los votos sellados en el momento del cierre.
Neutralidad	La plataforma recoge los votos y presenta los resultados. No aplica quórum ni mayorías ni proclama nada: eso corresponde a la mesa.



1.4. Definiciones

Término	Definición
Evento de votación	Sesión o proceso convocado (una asamblea, una consulta). Tiene fecha y hora de inicio y de fin, su propio censo y puede contener una o varias votaciones.
Votación	Cada pregunta que se somete a voto dentro de un evento, con sus opciones de respuesta.
Censo	Relación de colegiados habilitados para votar en un evento, obtenida del programa de gestión colegial (eColegios).
Votante telemático (online)	Colegiado del censo que se ha identificado con su certificado digital para votar a distancia.
Votante presencial	Colegiado del censo que ha sido acreditado a la entrada de la sala.
Lista de participación	Registro, por cada votación, de qué colegiados han votado. Equivale a la lista que firma el votante al depositar su papeleta.
Urna digital	Registro de los votos emitidos en cada votación, sin ningún dato del votante ni del orden de llegada.
Huella (hash)	Código que resume de forma única un contenido. Si el contenido cambia, aunque sea mínimamente, la huella cambia por completo.
Sellado de tiempo (OpenTimestamps)	Servicio público y gratuito que ancla una huella en la cadena de bloques de Bitcoin. Prueba que un contenido existía en un momento dado y que no ha cambiado desde entonces. Es el "precinto" de la urna.
Certificado FNMT	Certificado electrónico de persona física expedido por la Fábrica Nacional de Moneda y Timbre.
AutoFirma	Aplicación oficial y gratuita del Gobierno de España para firmar electrónicamente con un certificado.
OCSP	Servicio de la FNMT que confirma en tiempo real si un certificado es válido o ha sido revocado.
Lector de acceso	Herramienta de la plataforma, usada en un móvil o tableta, para acreditar a los asistentes en la sala escaneando su carné colegial digital o su DNI.



2. ROLES Y RESPONSABILIDADES

Cada persona que interviene en un proceso de votación tiene un papel definido y accede a la plataforma con sus propias credenciales. Cada perfil solo puede realizar las acciones que le corresponden, y las acciones relevantes quedan registradas con la persona que las realizó (ver apartado 11).

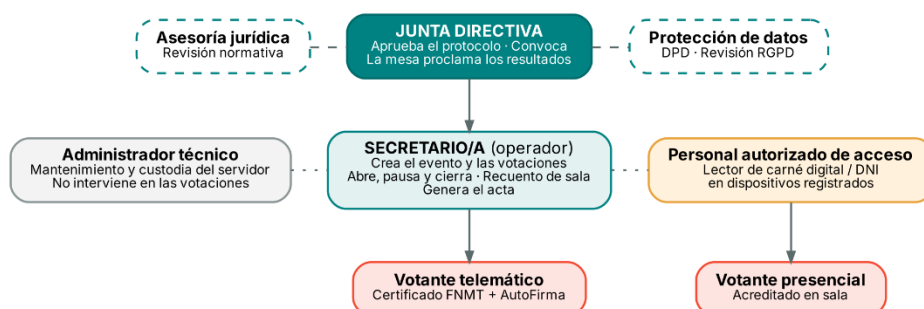


Figura 1. Organigrama de funciones en un proceso de votación.

Rol	Responsabilidades
Junta Directiva	Aprueba este protocolo y sus revisiones. Convoca cada proceso y fija las preguntas. Constituida en mesa, interpreta los resultados según los Estatutos (quórum, mayorías) y los proclama.
Secretario/a (operador de la votación)	Es el único perfil que gestiona las votaciones: crea el evento y fija sus criterios de censo, crea las votaciones, las abre, pausa y cierra, introduce el recuento de los votos emitidos en la sala, modera el chat y genera el acta de resultados. Puede designar a una persona de apoyo con su mismo perfil.
Personal autorizado de acceso	Personal del Colegio designado para acreditar a los asistentes a la entrada de la sala con el lector de acceso. Solo puede consultar si una persona está en el censo y registrarla como presencial. Trabaja con dispositivos que el Administrador técnico ha registrado previamente.
Administrador técnico	Mantiene la plataforma y el servidor, registra los dispositivos del lector y custodia los archivos históricos. No interviene en la gestión de las votaciones ni tiene perfil de secretario. Es la única persona con acceso al servidor.
Votante	Colegiado incluido en el censo. Es responsable de la custodia de su certificado digital y de disponer de AutoFirma en su equipo si vota a distancia.
Asesoría jurídica	Revisa la adecuación normativa del protocolo y asesora a la mesa ante cualquier impugnación.
Delegado de Protección de Datos	Valida el tratamiento de datos personales y redacta los textos informativos que se muestran en la plataforma.



3. ESQUEMA GENERAL DE FUNCIONAMIENTO

La figura 2 resume el ciclo completo de una votación, desde la preparación del evento hasta el archivo histórico. Los colegiados acceden por una de las dos vías, telemática o presencial. Ambas confluyen en la misma urna y en la misma lista de participación, y a partir del cierre siguen un tratamiento común.

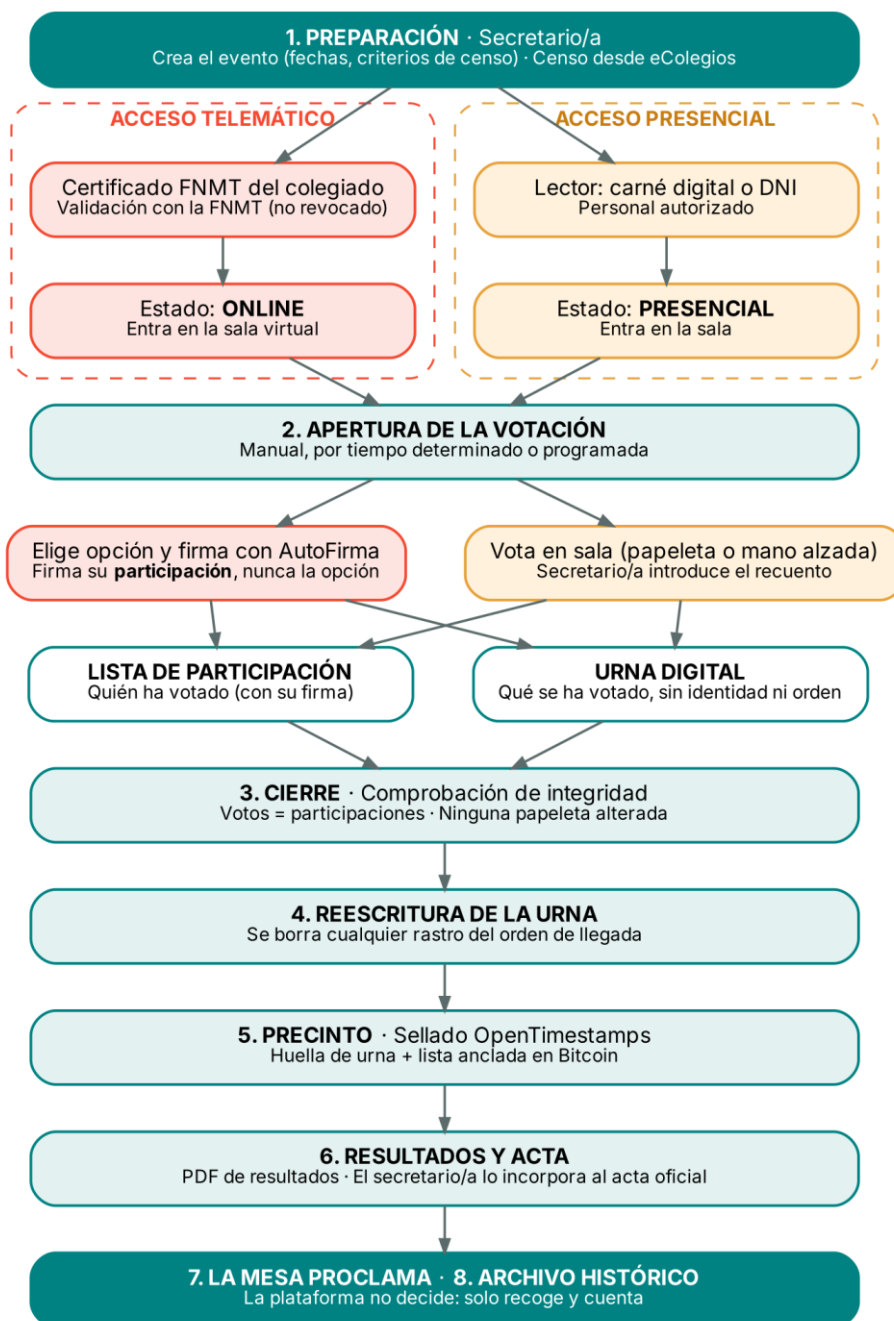


Figura 2. Ciclo de una votación.



En resumen, las fases son:

- **Preparación.** El secretario/a crea el evento, fija las fechas y los criterios de censo y prepara las votaciones.
- **Acceso.** Los colegiados se acreditan con su certificado digital (a distancia) o con el lector de acceso (en la sala).
- **Votación.** El secretario/a abre cada votación. Los votantes a distancia votan desde su dispositivo y la sala vota por el método que decida la mesa.
- **Cierre e integridad.** Al cerrar, el sistema comprueba que todo cuadra y que ningún voto ha sido alterado.
- **Reescritura de la urna.** Se elimina cualquier rastro del orden en que llegaron los votos.
- **Precinto.** La urna y la lista de participación se sellan con OpenTimestamps.
- **Resultados y acta.** El sistema presenta los resultados y genera el acta de resultados en PDF.
- **Proclamación y archivo.** La mesa proclama los resultados y el evento se conserva como archivo histórico.

4. EVENTOS Y ESCENARIOS DE VOTACIÓN

4.1. El evento de votación

Toda votación se celebra dentro de un **evento**. Un evento puede contener una o varias votaciones, por ejemplo los distintos puntos del orden del día de una asamblea. Al crear el evento, el secretario/a fija:

- **Fecha y hora de inicio y de fin.** Marcan cuándo pueden acceder los votantes a distancia, con independencia de que haya o no votaciones abiertas. Fuera de ese horario no es posible identificarse ni votar.
- **Criterios de censo:** qué colegiados pueden votar según su situación colegial y su estado de pago (ver 5.1).
- **Modalidad:** con retransmisión en directo o sin ella.

4.2. Modalidades de evento

	Asamblea en directo	Consulta telemática de varios días
Votantes	En la sala y a distancia, simultáneamente	Solo a distancia
Retransmisión de vídeo	Sí, visible para los votantes a distancia	No. Si no hay emisión, la ventana de vídeo no se muestra
Chat	Sí, moderado por el secretario/a	Solo se muestra cuando el secretario/a está conectado
Tipo de votación habitual	Manual o por tiempo determinado	Programada



4.3. Tipos de votación

Cada votación puede abrirse y cerrarse de tres formas:

Tipo	Funcionamiento
Manual	La votación no es visible para los votantes hasta que el secretario/a la abre, y permanece abierta hasta que la cierra.
Por tiempo determinado	El secretario/a fija una duración en minutos. Al abrirla, los votantes ven una cuenta atrás. Al agotarse el plazo, el servidor deja de admitir votos de forma automática.
Programada	Se fija una fecha y hora de apertura y de cierre. El servidor la abre y la cierra automáticamente, sin necesidad de que el secretario/a esté conectado. Es la forma prevista para las consultas de varios días.

4.4. Opciones de voto

- Cada votación tiene las opciones que fije el secretario/a, y el votante elige **una sola**.
- El sistema añade siempre la opción **"Voto en blanco"**, que es un voto válido.
- **Abstención:** se considera que se abstiene el votante acreditado que no emite voto en una votación. En la sala, la mesa puede contabilizar también abstenciones expresas al introducir el recuento.
- Los votantes **no ven resultados** mientras la votación está abierta.

4.5. Estados de una votación

Estado	Significado y reglas
Creada	Preparada pero no visible. Puede editarse o eliminarse.
Abierta	Visible para los votantes. Se admiten votos.
Pausada	El secretario/a la detiene temporalmente: deja de ser visible y no se admiten votos. Puede reanudarse. Los votos ya emitidos se conservan.
Finalizada	Cerrada de forma definitiva e irreversible . No admite más votos ni cambios. Requiere que se haya introducido el recuento de la sala.
Sellada	La urna y la lista de participación han sido precintadas con OpenTimestamps.
Confirmada	El sello ha quedado anclado en la cadena de Bitcoin (normalmente en pocas horas).

Una votación solo puede editarse o eliminarse si todavía no ha recibido ningún voto.
Una votación con votos no puede eliminarse: solo finalizarse, y figurará en el acta.



4.6. Votación simultánea presencial y telemática

En las asambleas en directo conviven las dos modalidades. Cada colegiado vota **por una sola vía** y el sistema lo garantiza mediante su estado en el evento (ver 5.2):

- El secretario/a abre la votación una sola vez y queda abierta a la vez para la sala y para los votantes a distancia.
- Los votantes a distancia votan desde su dispositivo mientras la votación esté abierta.
- En la sala se vota por el método que decida la mesa (papeleta o mano alzada) y el secretario/a introduce el recuento en la plataforma (ver apartado 7).
- La votación solo puede finalizarse cuando se ha introducido el recuento de la sala.
- Los votos de ambas vías se depositan en la **misma urna** y se cuentan juntos. El resultado muestra además el desglose de votos telemáticos y presenciales.

5. CENSO E IDENTIFICACIÓN DEL VOTANTE

5.1. Censo del evento

El censo se obtiene directamente de eColegios al configurar el evento, aplicando dos criterios que fija el secretario/a: la **situación colegial** (por defecto, ejerciente) y el **estado de pago** de las cuotas (por defecto, al corriente). De cada colegiado se toman únicamente su DNI, su nombre y sus apellidos.

- El censo puede actualizarse mientras no se haya abierto ninguna votación del evento. A partir de ese momento queda **fijado** y no puede modificarse.
- Cada actualización del censo y cada cambio en los criterios queda registrado en la auditoría con la persona que lo realizó.



5.2. Estados del votante

Cada colegiado del censo tiene un estado único en el evento:

Estado	Cuándo se alcanza	Consecuencia
No presente	Estado inicial de todo el censo.	Puede acreditarse por cualquiera de las dos vías.
Online	Al identificarse por primera vez con su certificado digital, dentro del horario del evento.	Vota a distancia. Ya no puede acreditarse en la sala.
Presencial	Al ser acreditado con el lector de acceso a la entrada de la sala.	Vota en la sala. Ya no puede identificarse a distancia.

Solo se puede pasar de **No presente** a Online o a Presencial. **No existe el paso entre Online y Presencial en ningún sentido.**

El cambio de estado se realiza en una única operación indivisible, de modo que dos intentos simultáneos (por ejemplo, entrar a distancia mientras se pasa por el lector) nunca pueden tener éxito los dos.

Si el personal de acceso registra a una persona por error, solo el Administrador Técnico puede devolverla al estado No presente, siempre que no haya participado todavía en ninguna votación. La corrección queda registrada en la auditoría con su motivo.

5.3. Acceso telemático

- El colegiado accede a la plataforma y su navegador le pide que elija su **certificado electrónico de la FNMT** de persona física.
- El sistema comprueba que el certificado es auténtico, que pertenece a un colegiado del censo y que su estado es No presente u Online.
- Consulta a la FNMT (**OCSP**) que el certificado está vigente y no revocado. **Solo se admite votar con un certificado verificado como válido.**
- Superadas las comprobaciones, el colegiado entra en la sala virtual (vídeo, chat y votaciones) y pasa a estado Online.
- La sesión se renueva automáticamente mientras la página permanece abierta. Si caduca o se pierde la conexión, basta con volver a identificarse: el votante conserva su estado y los votos ya emitidos.

La convocatoria indicará a los colegiados que pueden **probar AutoFirma** desde la página de acceso antes del inicio de la sesión.



5.4. Acceso presencial

- A la entrada de la sala, el personal autorizado escanea el **QR del carné colegial digital** o el **DNI** del colegiado, o teclea el número del documento.
- El lector solo funciona en **dispositivos registrados** previamente por la administración para ese uso.
- El sistema muestra si la persona está en el censo y su estado. Si está como No presente, el personal confirma la acreditación y pasa a Presencial.
- Si la persona ya está acreditada a distancia, el lector lo indica y no permite su acreditación en la sala.
- Cada acreditación queda registrada con su hora y el dispositivo que la realizó.

5.5. Información a los colegiados

Como un votante identificado a distancia ya no puede votar en la sala, la convocatoria advertirá expresamente que **identificarse con el certificado digital supone optar por el voto telemático para todo el evento**. Quien prefiera votar en la sala no debe acceder a la plataforma con su certificado.

6. EMISIÓN DEL VOTO TELEMÁTICO

6.1. Secuencia

- El votante elige una opción y pulsa "Emitir voto".
- El servidor genera un **código de autorización de un solo uso**, válido durante unos minutos.
- Se abre **AutoFirma** en el equipo o móvil del votante, que firma ese código con su certificado.
- La pantalla envía al servidor la firma y, por separado, la opción elegida.
- El servidor realiza todas las comprobaciones (ver 6.3), registra la participación y el voto **por separado**, y responde. El votante ve "Voto emitido".

6.2. Qué firma el votante y qué no

El votante **firma su participación, no su voto**. Lo firmado contiene la votación de que se trata, un identificador del votante, el momento y el código de un solo uso. **La opción elegida nunca forma parte de lo firmado**.

Es el equivalente digital a firmar en la lista de votantes al depositar la papeleta: la firma acredita, con plena validez, que esa persona ha votado en esa votación, pero no dice nada de lo que ha votado.



6.3. Comprobaciones antes de admitir un voto

El servidor solo admite un voto si se cumplen **todas** estas condiciones. Si falla cualquiera, el voto se rechaza y el votante recibe un aviso:

- La sesión del votante es válida y corresponde a ese evento.
- El código de autorización existe, no ha caducado y no se ha usado antes. Se consume en ese momento.
- La firma es válida y corresponde exactamente al código emitido.
- La firma se ha hecho con el **mismo certificado** con el que el votante se identificó, y ese certificado consta como válido ante la FNMT.
- El votante está en el censo de esa votación, está en estado Online y **no ha votado ya**. Esta comprobación es indivisible: dos envíos simultáneos nunca pueden contar dos veces.
- La votación está **abierta** y dentro de su horario.
- La opción elegida es una de las opciones de esa votación.

6.4. Dónde queda cada dato

Registro	Qué contiene	Qué NO contiene
Lista de participación	Quién ha votado en cada votación y su firma de participación.	La opción votada.
Urna digital	La opción elegida, un valor aleatorio y la huella del voto.	Ningún dato del votante, ni la fecha y hora, ni el orden de llegada.
Auditoría	Las acciones del secretario/a, del personal de acceso y del sistema (ver 11.1).	El contenido de los votos ni el momento en que vota cada persona.

El sistema no guarda la dirección IP ni datos del dispositivo del votante.



7. VOTO PRESENCIAL Y RECUENTO EN SALA

La mesa decide cómo vota la sala (papeleta, mano alzada u otro método admitido por los Estatutos). Al sistema solo le corresponde garantizar que **los votos de la sala correspondan exactamente a las personas acreditadas en ella**. Para ello:

- Con la votación abierta, el secretario/a introduce el recuento de la sala: votos a cada opción, votos en blanco y abstenciones.
- La suma debe ser **exactamente igual** al número de votantes presenciales acreditados en ese momento. El sistema no admite ni un voto más ni uno menos.
- El recuento se introduce **una sola vez por votación** y no puede modificarse después. El sistema registra quién lo introdujo y cuándo.
- Cada voto de la sala se deposita **uno a uno** en la urna, con el mismo formato que los telemáticos, y todos los presenciales quedan marcados como "ha votado" en esa votación.
- Una votación no puede finalizarse sin su recuento de sala si hay votantes presenciales acreditados.
- Un asistente que se acredita una vez introducido el recuento de una votación no participa en ella: solo cuenta en las votaciones cuyo recuento se introduzca después de su llegada.

8. SECRETO DEL VOTO

El secreto del voto se apoya en la misma idea que una votación tradicional con **lista, urna y precinto**:

Elemento	Votación tradicional	Plataforma
Lista	El votante firma en la lista al votar.	Lista de participación con la firma digital de participación.
Urn	Las papeletas se mezclan y no se sabe de quién es cada una.	Urn digital sin identidad ni orden, que se reescribe al cierre.
Precinto	La urna se precinta y se levanta acta.	Sellado de la urna y la lista con OpenTimestamps.

8.1. Separación entre quién vota y qué vota

La participación y el voto se guardan en **registros distintos que no comparten ningún dato**. La huella de cada voto se calcula a partir de la opción elegida y de un valor aleatorio propio, y no a partir de la firma ni de ningún dato del votante. Por eso, conocer la firma de una persona no permite localizar su voto.



8.2. Urna sin orden

Si la urna conservara el orden de llegada, bastaría con compararlo con el orden de las firmas para deducir el voto de cada persona. Por eso:

- Cada voto recibe un **identificador aleatorio**, que no sigue ningún orden.
- La urna **no guarda la fecha ni la hora** de los votos.
- La plataforma **no anota en la auditoría el momento en que vota cada persona**.
- El servidor de base de datos no mantiene registros cronológicos de las operaciones.

8.3. Reescritura de la urna al cierre

Las bases de datos conservan internamente, en sus ficheros, rastros técnicos del orden en que se escribieron los datos. Para eliminarlos, al cerrar cada votación y antes de precintarla, el sistema:

- Copia todos los votos a una urna nueva **en una única operación**, con identificadores nuevos y en un orden que no guarda relación con la llegada.
- Sobrescribe el contenido de la urna original con datos sin valor y fuerza su escritura en disco.
- Elimina la urna original y su fichero.

Las huellas de los votos no cambian con la reescritura, de modo que el precinto posterior es idéntico y verificable.

GARANTÍA DE SECRETO

Una vez cerrada la votación, **ni consultando la base de datos ni con acceso a sus ficheros es posible relacionar un voto con su votante ni con su orden de llegada**.

Mientras la votación está abierta, la protección es el control de acceso al servidor, restringido al administrador técnico. Un intento en ese momento sería además incompleto: no se sabe quién va a votar ni cuándo se cerrará la votación.



9. CIERRE, SELLADO Y RESULTADOS

9.1. Cierre de una votación

La votación se cierra cuando el secretario/a la finaliza o, en las votaciones por tiempo determinado y programadas, al vencer su plazo. El cierre es irreversible. A partir de ese momento el sistema inicia, de forma automática, la comprobación, la reescritura y el sellado.

9.2. Comprobación de integridad

Antes de precintar, el sistema recalcula la huella de cada voto y comprueba que:

- Ningún voto ha sido alterado desde que se emitió.
- Todas las opciones registradas son opciones válidas de la votación.
- El número de votos coincide con el número de participaciones registradas en la lista.

Si alguna comprobación falla, **la votación no se sella**, queda marcada como incidencia en la auditoría y el secretario/a es avisado para que lo traslade a la mesa (ver Anexo I).

9.3. Precinto con OpenTimestamps

Con las huellas de todos los votos se calcula una huella única de la urna y, del mismo modo, una huella única de la lista de participación. Ambas se combinan en una sola huella, que se envía a **OpenTimestamps**.

- En pocos minutos se obtiene un justificante provisional de los servidores públicos de OpenTimestamps.
- En unas horas, el sello queda **anclado en la cadena BlockChain de Bitcoin**. Desde el momento del envío de la huella a OpenTimestamps es imposible modificar un solo voto, añadirlo o quitarlo sin que la comprobación del precinto falle.
- El precinto no revela ningún dato: solo contiene huellas, de las que **no se puede reconstruir el contenido**.



9.4. Resultados

La plataforma presenta, para cada votación:

Dato	Cómo se obtiene
Votos por opción	Votos de la urna para cada opción (telemáticos y presenciales), con su desglose.
Votos en blanco	Votos a la opción "Voto en blanco". Son votos válidos.
Votos emitidos	Suma de los votos por opción y en blanco.
Abstenciones	Votantes acreditados que no han emitido voto, más las abstenciones expresas contabilizadas en la sala.
Votantes acreditados	Telemáticos y presenciales.
Censo y no presentes	Total del censo y colegiados que no se han acreditado por ninguna vía.

Las definiciones son las mismas en el panel del secretario/a y en el acta, y el sistema comprueba que **votos emitidos + abstenciones = votantes acreditados**. La plataforma **no aplica reglas de quórum ni de mayoría** y no proclama resultados: la mesa los interpreta conforme a los Estatutos.

10. ACTA DE RESULTADOS

Cuando todas las votaciones del evento están finalizadas y selladas, el secretario/a genera el **acta de resultados** en PDF. Contiene:

- Identificación del evento y fecha y hora de generación.
- Resumen del censo: habilitados, acreditados telemáticos, acreditados presenciales y no presentes.
- Por cada votación: pregunta, tipo, horas de apertura y cierre, resultados con el desglose telemático y presencial, abstenciones y porcentajes.
- Datos del precinto de cada votación: huellas selladas, fecha del sellado. El estado de la confirmación en Bitcoin no es posible incluirlo ya que puede tardar horas o días en comprobarse.
- Persona que actuó como secretario/a y, en su caso, personas de apoyo.

La generación del acta **cierra el evento**: a partir de ese momento no se puede realizar ningún cambio en sus votaciones. La huella del PDF queda registrada en la auditoría, de modo que cualquier copia puede compararse con el original.

El acta de resultados no se firma electrónicamente en la plataforma. El secretario/a la **incorpora al acta oficial de la sesión**, que firma conforme a los Estatutos. Si fuera necesario regenerarla por un error material, solo podrá hacerlo el Administrador Técnico, y la regeneración quedará registrada con su motivo.



11. AUDITORÍA Y VERIFICACIÓN

11.1. Registro de actuaciones

La plataforma registra con fecha, hora y autor:

- Las acciones del secretario/a: creación y cambios del evento y del censo, creación, apertura, pausa y cierre de votaciones, recuento de la sala, moderación del chat y generación y descarga del acta.
- Las acreditaciones del personal de acceso, con el dispositivo utilizado.
- Las acciones automáticas del sistema: verificaciones de certificados con la FNMT, comprobaciones de integridad, sellados y confirmaciones.
- Los intentos rechazados (firmas no válidas, accesos fuera de censo).

El registro de actuaciones **nunca contiene el contenido de los votos ni el momento en que vota cada persona**. Se archiva junto con el evento.

11.2. Verificación independiente

Para cada votación sellada, la plataforma permite descargar el **justificante de OpenTimestamps** y la **huella sellada**. Con ellos, cualquier auditor puede comprobar con el cliente oficial de OpenTimestamps, o en opentimestamps.org, sin depender del Colegio, en qué fecha quedó sellada esa huella en la cadena de Bitcoin.

Además, el sistema conserva para cada voto y cada participación su posición dentro de la huella sellada, de modo que puede demostrarse que un voto o una participación concretos formaban parte de lo precintado.

11.3. Qué puede comprobar un auditor

Un auditor **puede comprobar**:

- Que los votos y la lista de participación no han cambiado desde el cierre, y la fecha exacta del precinto.
- Que el número de votos coincide con el de participaciones.
- Que cada participación telemática está firmada con un certificado FNMT válido de un colegiado del censo.
- Que los resultados del acta coinciden con el contenido de la urna sellada.

En cambio, **no puede averiguar** qué ha votado una persona concreta ni en qué orden llegaron los votos. Nadie puede.



12. GARANTÍAS DE SEGURIDAD INTERNA

Este apartado responde a las preguntas que con más frecuencia se plantean sobre la posibilidad de manipulación desde dentro de la organización.

12.1. ¿Puede alguien del Colegio saber qué ha votado una persona?

No. El secretario/a no tiene acceso a la urna ni a la base de datos. El administrador técnico, que sí tiene acceso al servidor, encuentra la participación y el voto en registros separados que no comparten ningún dato ni orden de inserción. Una vez cerrada la votación, la urna se reescribe y desaparece cualquier rastro del orden de llegada (ver apartado 8).

12.2. ¿Se pueden añadir votos falsos?

No sin que se detecte. Cada voto telemático exige una firma de participación hecha con el certificado FNMT válido de un colegiado del censo, y esa firma queda en la lista de participación. Para añadir un voto haría falta el certificado de otra persona, y su firma dejaría un rastro identificable. El número de votos de la urna debe coincidir con el de participaciones o la votación no se sella. Los votos de la sala están limitados exactamente al número de acreditados.

12.3. ¿Se puede modificar un voto o un resultado después?

No. La comprobación de integridad detecta cualquier alteración antes del precinto, y después del precinto cualquier cambio, por mínimo que sea, hace que la verificación con OpenTimestamps falle. El acta queda identificada por su huella.

12.4. ¿Puede una persona votar dos veces?

No. Cada colegiado tiene un único estado en el evento (online o presencial, nunca los dos) y un único "ha votado" por votación, que se marca en una operación indivisible. Cada código de autorización solo sirve una vez.

12.5. ¿Se puede votar sin un certificado válido?

No. Solo se admiten certificados de persona física de la FNMT, verificados en tiempo real ante la propia FNMT. Un certificado revocado, caducado o no verificado no permite votar.

12.6. Límites que conviene conocer

Ningún sistema es invulnerable. Estos son los riesgos residuales conocidos y cómo se acotan:

- **Votación abierta.** Durante el tiempo en que una votación está abierta, la protección depende del control de acceso al servidor (ver apartado 8).
- **Copias técnicas residuales.** Tras la reescritura, ciertos registros internos de la base de datos y del disco pueden conservar temporalmente fragmentos hasta que se sobrescriben con la actividad normal. Recuperarlos exigiría acceso de



administrador al servidor y un análisis forense, o acceso al hardware del proveedor, en el momento exacto de cerrar una votación.

- **Entorno del votante a distancia.** Como en cualquier voto no presencial, el Colegio no puede garantizar que el votante esté solo al votar. La custodia del certificado es responsabilidad de su titular.
- **Servicios externos.** El voto telemático depende de la FNMT, de AutoFirma y de la conexión a internet. Las actuaciones ante su fallo se recogen en el Anexo I.

12.7. Reglas operativas

- El acceso al servidor está restringido al administrador técnico, con autenticación reforzada.
- No se realizan copias de seguridad de la base de datos ni copias completas del servidor mientras haya una votación abierta.
- El servidor de base de datos funciona sin registros cronológicos de operaciones.
- Los dispositivos del lector se registran antes de cada evento y se dan de baja cuando dejan de usarse.
- Antes de cada proceso oficial se realiza una prueba técnica completa con un evento de prueba, que después se elimina.

13. MARCO LEGAL Y PROTECCIÓN DE DATOS

13.1. Marco normativo

- **Reglamento (UE) n.º 910/2014 (eIDAS)**, que regula la identificación electrónica y los servicios de confianza, incluida la firma electrónica avanzada.
- **Ley 6/2020, de servicios electrónicos de confianza**, que completa la aplicación de eIDAS en el ordenamiento jurídico español.
- **Ley 2/1974, de Colegios Profesionales**, que admite el uso de medios telemáticos en los órganos colegiados.
- **Ley 10/2003, de Colegios Profesionales de Andalucía**, que respalda el uso de medios electrónicos en el funcionamiento colegial.
- **Estatutos del Colegio**, artículos 29.5, 34.3 y 49.3.w, que permiten el voto telemático siempre que se garanticen la identidad, el secreto del voto, la integridad del proceso y la posibilidad de auditoría.
- **Reglamento (UE) 2016/679 (RGPD)** y **Ley Orgánica 3/2018 (LOPDGDD)**, de protección de datos personales.

13.2. Firma electrónica y validez

La participación de cada votante a distancia se acredita con una **firma electrónica avanzada** realizada con su certificado de la FNMT mediante AutoFirma. Esa firma vincula de forma única a su titular y no puede ser repudiada. La integridad de los votos se garantiza por separado, con su huella y el precinto de OpenTimestamps. Así se cumplen a la vez la acreditación de la identidad y el secreto del voto.



13.3. Protección de datos personales

- **Minimización.** Del censo se toman solo el DNI, el nombre y los apellidos. Del votante a distancia se conservan además su certificado y el resultado de su verificación. No se registran la dirección IP ni los datos del dispositivo.
- **Separación.** Los datos de identidad nunca se guardan junto al contenido de los votos.
- **Conservación.** Cada evento se conserva como **archivo histórico** de los órganos colegiales. Al terminar el proceso, el evento completo (datos, acta y auditoría) se exporta a un archivo con su huella de integridad y se retira del sistema activo. El archivo puede restaurarse si es necesario y vuelve a generar exactamente las mismas huellas, de modo que el precinto y la auditoría siguen siendo verificables. El plazo y las condiciones de conservación quedan sujetos al criterio del Delegado de Protección de Datos.
- **Acceso.** Los archivos históricos se custodian en el servidor del Colegio con acceso restringido al administrador técnico, y solo se restauran a petición de la Junta Directiva o por requerimiento judicial.
- **Información.** La plataforma muestra los textos informativos que elabore el Delegado de Protección de Datos antes de que el votante se identifique.

13.4. Participación de las asesorías

La **asesoría jurídica** del Colegio ha revisado el sistema y respalda este protocolo. El **Delegado de Protección de Datos** revisará el tratamiento de datos personales antes de la primera votación oficial. Sus indicaciones se incorporarán a la plataforma y, si afectan a este documento, a una nueva edición.

14. APROBACIÓN, PUESTA EN MARCHA Y REVISIÓN

14.1. Aprobación

Este protocolo entra en vigor tras su aprobación por la Junta Directiva, que constará en acta. Cualquier cambio sustancial en el funcionamiento del sistema requerirá una nueva edición aprobada del mismo modo.

14.2. Prueba piloto

Antes de la primera votación oficial se realizará una **prueba piloto** con una consulta no vinculante, preferentemente con la propia Junta Directiva, para validar la operativa técnica y organizativa y la experiencia de uso.



14.3. Preparación de cada proceso

Momento	Actuación	Responsable
Convocatoria	Preguntas, modalidad del evento, fechas e instrucciones para votar a distancia, con la advertencia de que identificarse con el certificado supone optar por el voto telemático (5.5) y la invitación a probar AutoFirma.	Junta Directiva / Secretario/a
Días previos	Creación del evento, revisión del censo, registro de los dispositivos del lector y prueba técnica completa.	Secretario/a / Administrador técnico
Durante el proceso	Acreditación en sala, apertura y cierre de votaciones, recuento de la sala, atención a incidencias.	Secretario/a / Personal de acceso
Cierre	Comprobación del sellado, generación del acta de resultados e incorporación al acta oficial. Proclamación por la mesa.	Secretario/a / Mesa
Posterior	Exportación del evento al archivo histórico y baja de los dispositivos del lector.	Administrador técnico

14.4. Revisión del protocolo

El protocolo se revisará tras la prueba piloto, tras cualquier incidencia relevante y, en todo caso, cuando cambie la normativa aplicable o el funcionamiento del sistema.



ANEXO I. CRITERIOS DE ACTUACIÓN ANTE INCIDENCIAS

ANEXO INDEPENDIENTE

Este anexo recoge una propuesta de criterios de actuación. Es independiente del resto del protocolo: puede modificarse o suprimirse sin afectar a los demás apartados.

Ante cualquier incidencia, el secretario/a informa a la mesa, que decide. Toda incidencia y la decisión adoptada constan en el acta oficial de la sesión.

Incidencia	Actuación propuesta
Un votante pierde la conexión.	Vuelve a entrar identificándose con su certificado. Conserva su estado y sus votos ya emitidos, y puede votar en las votaciones que sigan abiertas. Si una votación se cerró durante su desconexión, cuenta como abstención en ella.
AutoFirma falla en el equipo del votante.	Puede reintentarlo (cada intento genera un código nuevo) o votar desde otro equipo o móvil con su certificado. No existe una vía alternativa de voto ni puede pasar a votar en la sala. Si no consigue firmar la participación, contará como abstención en la votación.
El voto se registró, pero el votante no recibió la confirmación.	Al recargar la página, la votación aparece como "Voto emitido". La lista de participación es la referencia ante cualquier duda.
Caída general de la plataforma o de un servicio necesario (FNMT, servidor, conexión) con una votación abierta.	El secretario/a pausa la votación. Si el servicio se restablece en un plazo razonable, se reanuda: los votos ya emitidos se conservan y nadie puede votar dos veces. En las votaciones por tiempo determinado, la mesa decide la duración restante. Si no se restablece, la mesa decide aplazar la votación o celebrarla solo en la sala, haciéndolo constar en acta.
Falla internet en la sala.	El lector admite la introducción manual del DNI cuando vuelve la conexión. Si no es posible, el personal anota a los asistentes en una lista y los acredita en cuanto se restablezca, siempre antes de introducir el recuento de la votación afectada.
Error del personal al acreditar a una persona.	El administrador técnico la devuelve a No presente, siempre que no haya participado en ninguna votación, y anota el motivo (5.2).



Incidencia	Actuación propuesta
Falla la comprobación de integridad al cerrar.	La votación no se sella. El administrador técnico analiza la causa y la mesa decide si se repite la votación. La incidencia queda en la auditoría.
Falla el sellado con OpenTimestamps.	El resultado es válido, pero el precinto queda pendiente. El sistema lo reintenta y, si no lo consigue, el administrador técnico lo relanza. Este es un proceso de sellado que no interfiere con los resultados.
Un colegiado afirma haber votado y no consta, o al revés.	Se consulta la lista de participación y su firma, sin acceder en ningún caso al contenido del voto. La mesa resuelve con el asesoramiento de la asesoría jurídica.
Error material en el acta de resultados.	El administrador técnico la regenera dejando constancia del motivo, antes de incorporarla al acta oficial (apartado 10).