

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	DTI-UDSI-INF-2026-020
	FECHA: 19-07-2026
GESTIÓN INTERNA DE DESARROLLO DE SISTEMAS INFORMÁTICOS	
INFORME SOBRE LA SEGURIDAD DEL PROCESO DE VOTACIÓN, EL ACTA DE ESCRUTINIO Y LA PUBLICACIÓN DE RESULTADOS	

1. Objeto del presente informe

El presente documento tiene por finalidad explicar, en términos claros y formales, de qué manera el sistema informático de participación ciudadana garantiza:

1. La identidad y habilitación de quien vota.
2. El secreto del sufragio.
3. La imposibilidad de votar más de una vez.
4. La preservación íntegra de los votos emitidos hasta el cierre del proceso.
5. La generación de un acta de escrutinio única, firmada e inmodificable.
6. La publicación transparente de los resultados y la determinación del ganador.

Este informe no sustituye un peritaje forense ni un dictamen técnico-pericial; describe el diseño y los controles implementados en el sistema, a fin de que un profesional del derecho pueda comprender el grado de seguridad y de trazabilidad del proceso.

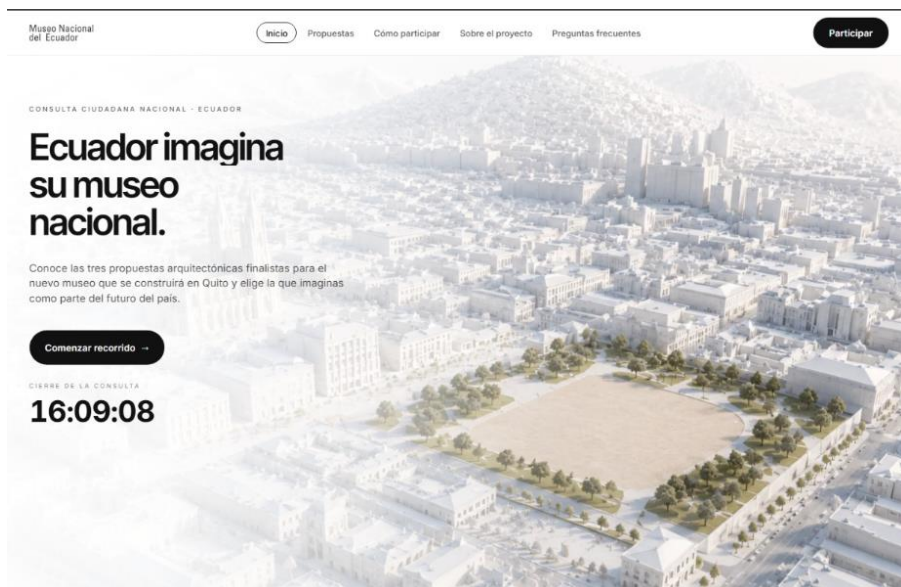
2. Naturaleza del proceso

Se trata de un proceso de participación ciudadana por medios electrónicos, en el cual:

- El ciudadano acredita su identidad ante el sistema.
- El sistema verifica, contra el Registro Civil (a través de los servicios oficiales del Ministerio de Telecomunicaciones y de la Sociedad de la Información — MINTEL), que la persona reúne las condiciones para participar.
- El ciudadano emite un voto a favor de una de las opciones habilitadas.
- Durante toda la vigencia del proceso, el contenido del voto permanece cifrado (ilegible para administradores y terceros).
- Solo al cierre formal, una autoridad autorizada ejecuta el escrutinio, que descifra, cuenta, genera el acta y publica los resultados.

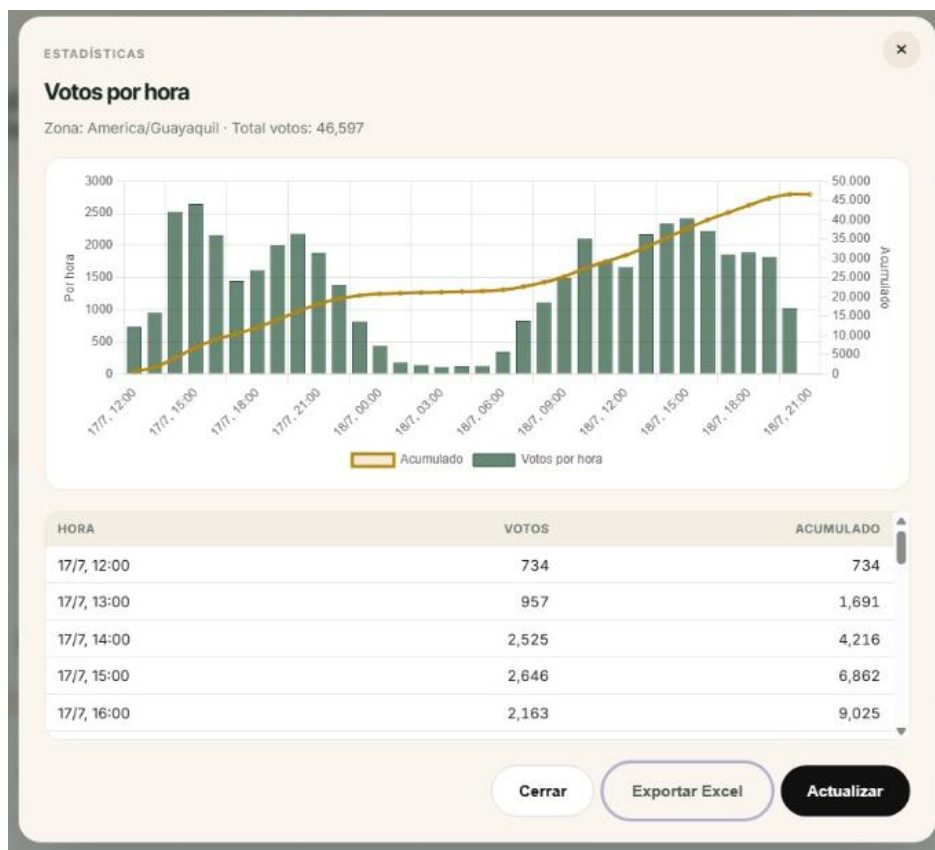
El sitio web o aplicación móvil actúa únicamente como pantalla de interacción. Toda decisión relevante (quién puede votar, si ya votó, qué se guarda y cómo se cuenta) la toma el servidor, no el dispositivo del ciudadano.

El sistema muestra una cuenta regresiva sobre el límite para ejecutar la votación, luego de este ya no es posible realizar el voto.



Pantalla inicial de Portal de voto

Existe un reporte donde se puede ver la cantidad de votantes, es necesario mencionar que el encriptado no permite ver por cual ha votado, solo permite ver el número total de registros en el sistema.



Reporte por horas número total de votantes

3. Seguridad implementada en el proceso de voto

3.1. Verificación de identidad

Antes de votar, el ciudadano debe suministrar su número de cédula y su fecha de nacimiento. El sistema consulta los datos oficiales del Registro Civil y aplica, entre otras, las siguientes reglas:

Condición	Efecto si no se cumple
La cédula existe en el Registro Civil	No se habilita
La fecha de nacimiento coincide exactamente	No se habilita
Edad mínima (dieciséis años o más)	No se habilita
Nacionalidad ecuatoriana	No se habilita
La persona no figura como fallecida	No se habilita

Si alguna condición falla, el ciudadano recibe un rechazo genérico, sin detallar el motivo específico, a fin de no facilitar intentos de suplantación o de prueba de datos ajenos.

Importante: Las credenciales de acceso a los servicios del Registro Civil nunca se entregan al navegador ni a la aplicación del ciudadano; permanecen exclusivamente en el servidor.

3.2. Credencial temporal de un solo uso (sesión de votación)

Una vez habilitado, el ciudadano recibe una credencial temporal (token de sesión de votación) con las siguientes características:

- Tiene un tiempo de vida corto (del orden de minutos).
- No contiene la cédula, el nombre ni otros datos personales.
- Sirve únicamente para obtener la papeleta y emitir el voto.
- Se invalida de inmediato al emitir el voto, de modo que no pueda reutilizarse.
- Es independiente de las credenciales de los funcionarios del sistema interno (backoffice); el ciudadano no ingresa como “usuario administrativo”.

En términos jurídicos prácticos: es comparable a un boleto de acceso de una sola oportunidad al acto de votar, no a una identificación permanente.

3.3. Secreto del voto (separación de identidad y elección)

El sistema se diseñó de modo que no exista un lugar único en el que figuren juntos, en claro, *quién* votó y *por qué opción* votó.

Existen tres registros separados:

1. Persona habilitada — Consigna que una persona (identificada mediante un *código derivado* de su cédula, no mediante la cédula en texto legible) fue validada y, en su caso, que ya votó. No guarda la opción elegida.
2. Voto cifrado — Consigna la elección del ciudadano, pero en forma encriptada. No guarda la identidad de la persona.

3. Vínculo técnico — Relaciona de forma operativa la sesión de votación con el voto emitido, sin almacenar la cédula ni la opción en texto claro. Sirve para impedir un segundo voto.

Esta separación es la base del secreto del sufragio en el diseño del sistema.

PARTICIPACIÓN

Voto registrado

Su participación ha sido registrada de forma anónima.
Gracias por imaginar el futuro Museo Nacional del Ecuador.

Su participación ha sido registrada. Puede responder una encuesta breve (opcional).

Cuéntanos qué te gustaría encontrar en el futuro Museo Nacional. Es opcional y te tomará menos de un minuto.

Ayúdanos a diseñar el museo

Ahora no

Pantalla de confirmación de voto registrado

3.4. Cifrado de cada voto

Cada voto se almacena cifrado con un algoritmo de cifrado autenticado de alto estándar (AES-256-GCM). Ello implica, en lenguaje sencillo:

- Mientras el proceso está abierto, ni funcionarios ni administradores de base de datos pueden leer “por quién votó” alguien.
- Cualquier alteración del contenido cifrado se detecta al momento del escrutinio, porque el sistema verifica una huella digital de integridad asociada a cada voto.

3.5. Un solo voto por persona (anti-doble participación)

El sistema impide que una misma persona habilitada vote dos veces en el mismo proceso. Si intenta hacerlo, el segundo intento es rechazado. El vínculo técnico y el registro de “ya votó” actúan de forma conjunta a este efecto.

3.6. Orden aleatorio de opciones en la papeleta

Las opciones se presentan al ciudadano en un orden distinto por sesión, determinado por el servidor. Ello reduce el sesgo de “la primera opción de la lista” y garantiza que el dispositivo del ciudadano no manipule el orden.

3.7. Rol pasivo de la interfaz del ciudadano

La interfaz (página web o aplicación):

- Sí captura cédula y fecha de nacimiento, muestra opciones y confirma la recepción del voto.
- No decide si la persona es elegible, no cifra el voto, no reordena las opciones por su cuenta y no puede declarar por sí sola que el voto fue válido.

La autoridad del acto reside en el servidor.

3.8. Controles adicionales de seguridad operativa

- Limitación de intentos repetidos (protección frente a ataques masivos o de prueba contra el punto de validación de identidad).
- Registro de eventos de auditoría (quién habilitó, cuándo se votó, cuándo falló un escrutinio, etc.), sin exponer datos personales innecesarios en los logs.
- Separación entre las APIs abiertas al ciudadano y las APIs reservadas a la autoridad de escrutinio (esta última protegida por clave administrativa independiente).

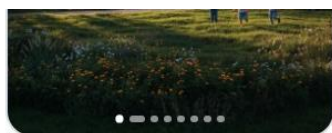
4. Cierre del proceso y generación del acta de escrutinio

4.1. Momento en que puede realizarse el escrutinio

El escrutinio no se ejecuta de forma automática al emitir cada voto. Solo puede realizarse cuando:

- Ha finalizado la ventana temporal del proceso de participación, o
- Una autoridad autorizada ordena el cierre anticipado de manera expresa y controlada.

Hasta ese momento, los votos permanecen cifrados y no existe “tabla de resultados en vivo” elaborada a partir del descifrado.



PROPUESTA 01 - ARQUITECTURA Y LERA

Topografías de Memoria

Un paisaje de memoria donde el visitante descubre cómo se investigan, conservan y ponen en valor las colecciones.



PROPUESTA 02 - MARIO CUCINELLA ARCHITECTS

Paisaje urbano transitable

El edificio se puede recorrer incluso sin ingresar al museo; el recorrido exterior es parte de la experiencia.



PROPUESTA 03 - SANAA

Living Strata - Estratos Vivos

El museo como organismo vivo: arquitectura, agua, vegetación y espacio público en un solo ecosistema.

[← Volver al recorrido](#)

La consulta ciudadana ha finalizado. Ya no es posible elegir una propuesta.

Consulta finalizada

Pantalla de cierre de votaciones (fin de votaciones)

4.2. Quién puede ejecutar el escrutinio

La operación de cierre y escrutinio está restringida a un canal administrativo protegido (clave de autoridad), distinto de las rutas públicas por las que vota el ciudadano.

Queda registrado:

- La identidad operativa del sujeto que ejecutó el escrutinio.
- La dirección IP de origen de la operación.
- Un identificador de correlación del procedimiento.
- La fecha y hora del escrutinio.

```
kubeconfig entry generated for gke-mit-apps-dev.
izquierdo@cloudshell:~ (mtop-sitopv2-dev)$ POD=$(kubectl get pod -n default -l app=voting-service -o jsonpath='{.items[0].metadata.name}')
KEY=$(kubectl exec -n default "$POD" -- printenv VOTING_ADMIN_API_KEY)
PORT=$(kubectl exec -n default "$POD" -- printenv SERVER_PORT)
PORT=${PORT:-9016}

kubectl exec -n default "$POD" -- \
  curl -sS -X POST \
  "http://localhost:${PORT}/api/v1/admin/procesos/770e8400-e29b-41d4-a716-446655440000/cerrar-escrutinio" \
  -H "Content-Type: application/json" \
  -H "X-Admin-API-Key: ${KEY}" \
  -H "X-Correlation-Id: ${uidgen}" \
  -d '{}'

-bash: uidgen: command not found
{"codigoRespuesta": "1", "mensajeRespuesta": "Acta de resultados generada", "objeto": {"actaId": "59bc412e-0781-481d-8811-0bd8b81cdc81", "procesoParticipativoId": "770e8400-e29b-41d4-a716-446655440000", "hashIntegridadActa": "e5abe68a8216020c60a5fa6a9caca482cf9350b9e1016b592cfd348620ef5918", "totalVotosValidos": 50681, "fechaEscrutinio": "2026-07-19T14:31:26.373284394Z", "estadoProceso": "FINALIZADO"}}
izquierdo@cloudshell:~ (mtop-sitopv2-dev)$
```

Comandos ejecutados para el cierre de escrutinio

4.3. Verificación de cuadre (consistencia previa al conteo)

Antes de descifrar voto alguno, el sistema comprueba que cuadren tres magnitudes del mismo proceso:

1. Cantidad de votos cifrados almacenados.
2. Cantidad de vínculos técnicos de votación.
3. Cantidad de personas habilitadas marcadas como "ya votaron".

Si estas cifras no coinciden, el escrutinio se detiene y no se genera acta. Este control equivale, en espíritu, a un cuadre de urna: no se cuenta si el número de sobres no coincide con el registro de votantes.

4.4. Verificación, descifrado y tabulación

Superado el cuadre, el sistema procede voto por voto a:

1. Recalcular y verificar la huella de integridad de cada voto cifrado (detección de manipulación).
2. Descifrar la opción elegida.
3. Acumular los votos por cada opción válida.
4. Tratar como nulos los votos que no correspondan a una opción activa o que no puedan descifrarse correctamente.
5. Verificar nuevamente que la suma de votos válidos más nulos sea igual al universo de votos cifrados.

4.5. Contenido del acta

El acta de resultados (cabecera y detalle) deja constancia, entre otros elementos, de:

- Identificación del proceso participativo.
- Fecha de cierre de la votación y fecha del escrutinio.
- Totales de: personas habilitadas, votantes, votos cifrados, votos válidos y votos nulos.
- Desglose por opción: nombre (etiqueta) de la opción, cantidad de votos y porcentaje.
- Una huella raíz que ancla el universo de votos escrutados.
- Una huella de integridad del acta calculada sobre el contenido íntegro y ordenado del documento.
- Una firma digital asociada a dicha huella, generada con clave asimétrica del servicio de escrutinio.
- Datos de trazabilidad de la ejecución (quién ejecutó, IP, correlativo).

Además, el detalle del acta guarda un retrato (snapshot) del nombre de cada opción en el momento del escrutinio, de modo que un cambio posterior en el catálogo de opciones no altere el texto histórico del acta.

4.6. Inmutabilidad del acta

Una vez generada y guardada el acta:

- El sistema no admite más de un acta por proceso.
- En la base de datos están configurados mecanismos que prohíben modificar o eliminar los registros del acta y de su detalle. Cualquier intento de actualización o borrado es rechazado por el propio motor de datos.
- El proceso pasa al estado FINALIZADO.

En términos prácticos: el acta funciona como un documento electrónico cerrado, no como una hoja de cálculo editable.

4.7. Unicidad del procedimiento

Si el escrutinio ya se completó y existe acta, una nueva solicitud de cierre es rechazada. Si el escrutinio falla a mitad de camino, el sistema deja el proceso en un

estado de cierre controlado, registra el fallo en auditoría y no deja un acta parcial publicada como definitiva.

5. Publicación de resultados y determinación del ganador

5.1. Cómo se muestran los resultados

Tras el escrutinio exitoso, cualquier interesado puede consultar el acta a través de un canal público de consulta (sin necesidad de credenciales de funcionario), el cual entrega:

- Nombre del proceso.
- Fecha del escrutinio.
- Totales generales (habilitados, votantes, votos válidos, nulos).
- Tabla de resultados por opción (votos y porcentaje).
- Huellas de integridad y firma digital del acta (elementos de verificación).
- Indicación del ganador, según la regla descrita más abajo.

La interfaz de consulta presenta estos datos de forma legible; la fuente de verdad es el acta almacenada e inmutable, no un recálculo mutable en la pantalla.

5.2. Determinación del ganador

El sistema declara ganadora a la opción que obtuvo el mayor número de votos válidos.

Reglas complementarias:

- Si varias opciones empatan en el máximo, el sistema lo señala expresamente como empate (no oculta la existencia del empate).
- Si no hay votos válidos, no se declara ganador.

Resultado a consignar en el presente informe

> Opción ganadora: Mario Cucinella Architects

> Total de votos del ganador: 21,047 votos

> ¿Existió empate? No

> Referencia del acta (hash de integridad):

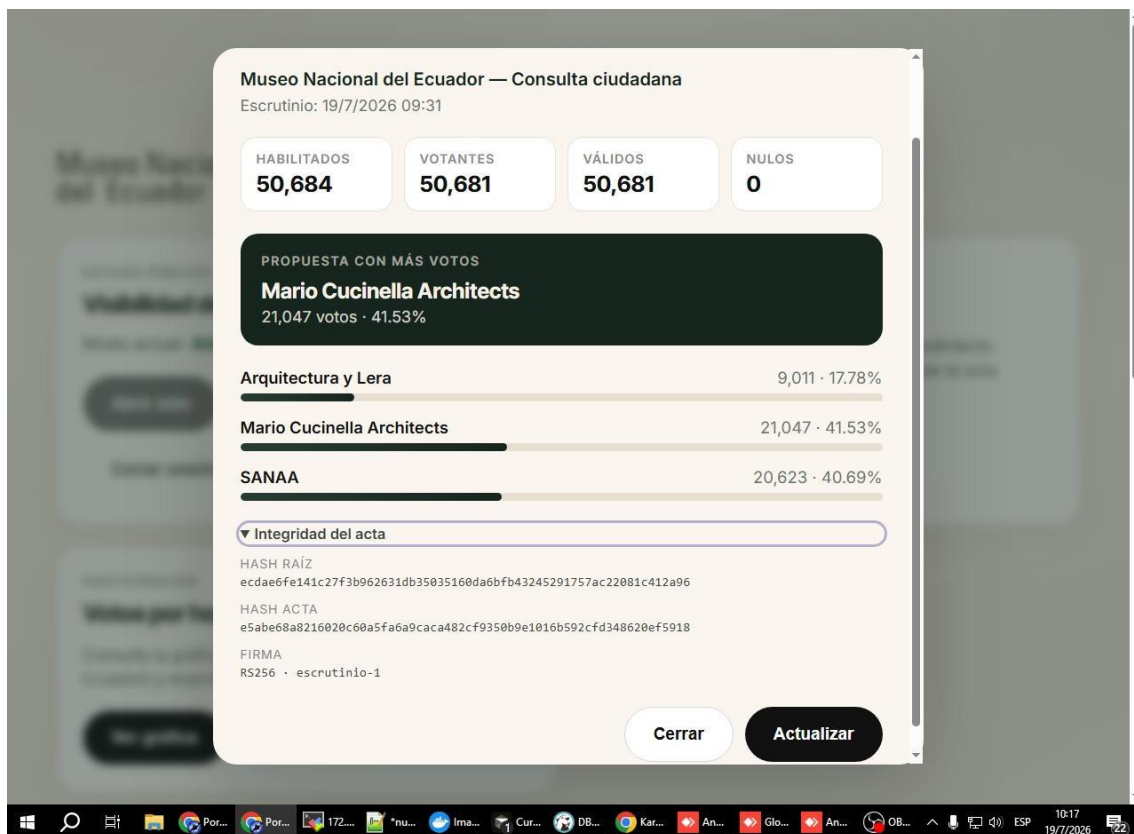
Hash raíz:

ecdae6fe141c27f3b962631db35035160da6bfb43245291757ac22081c412a96

Hash acta:

e5abe68a8216020c60a5fa6a9caca482cf9350b9e1016b592cfd348620ef5918

Firma: RS256 · escrutinio-1



Pantalla de administración muestra los resultados del escrutinio

5.3. Valor de las huellas y de la firma digital para el fedatario

Sin entrar en detalles criptográficos, conviene retener lo siguiente:

Elemento	Función jurídica-práctica
Huella de integridad de cada voto	Permite detectar si un voto individual fue alterado antes del conteo
Huella raíz de votos	Vincula el resultado al conjunto completo de votos escrutados
Huella de integridad del acta	Si alguien modifica cifras o etiquetas del acta, la huella deja de coincidir
Firma digital del acta	Atestigua que la huella del acta fue generada por la clave de firma del servicio de escrutinio, en el momento del cierre

Cualquier discrepancia entre el documento consultado públicamente y estos valores de control sería indicio de manipulación o de copia no auténtica.

6. Cómo se previno la manipulación de los datos

A modo de síntesis, las barreras contra la manipulación pueden agruparse así:

6.1. Durante la votación

Riesgo	Control implementado
Suplantación de identidad	Cruce con Registro Civil y coincidencia de fecha de nacimiento
Voto de quien no reúne requisitos	Reglas de elegibilidad aplicadas solo en el servidor
Doble voto	Registro de “ya votó” + vínculo técnico + token de un solo uso
Lectura del voto por terceros o funcionarios	Voto almacenado cifrado; identidad y elección separadas
Alteración del voto guardado	Huella de integridad verificada en el escrutinio
Manipulación desde la pantalla del ciudadano	El frontend no decide validez ni guarda el voto en claro en el servidor

6.2. En el escrutinio y el acta

Riesgo	Control implementado
Contar sin que cuadre la “urna”	Cuadre obligatorio entre votos, vínculos y votantes
Generar resultados inventados sin votos reales	El conteo deriva únicamente del descifrado de los votos almacenados
Modificar el acta después de publicada	Prohibición técnica de alterar o borrar el acta; un solo acta por proceso
Sustituir cifras en una copia	Huella de integridad + firma digital verificables
Ejecución por persona no autorizada	Canal administrativo aparte, con clave de autoridad y auditoría
Reejecutar el escrutinio para “cambiar” el resultado	Rechazo si ya existe acta; proceso en estado finalizado

6.3. Limitación honesta del alcance

Ningún sistema electrónico elimina por sí solo todos los riesgos del mundo físico (por ejemplo, coerción del votante frente a su propia pantalla, o compromiso extremo de la infraestructura completa). Lo que este diseño **sí** aporta, de manera documentable, es:

- Trazabilidad.
- Secreto del voto frente a administradores durante la vigencia del proceso.
- Unicidad del voto.
- Cuadre previo al conteo.
- Acta única, firmada e inmutable.

- Publicación verificable de resultados y ganador.

7. Conclusión

El proceso de participación ciudadana implementado en SITOP combina:

1. **Identificación oficial** del ciudadano mediante Registro Civil.
2. **Secreto del sufragio** mediante cifrado y separación de identidad y elección.
3. **Unicidad** del voto.
4. **Escrutinio controlado** solo al cierre, con cuadre previo.
5. **Acta de resultados única, firmada digitalmente e inmodificable.**
6. **Publicación abierta** de totales, desglose por opción y declaración del ganador (o del empate).

Para efectos de una diligencia notarial o de fe pública, se recomienda anexar o contrastar:

- La consulta pública del acta del proceso (incluyendo huella de integridad y firma digital).
- El nombre exacto de la opción ganadora y sus totales, tomados de esa acta.
- La constancia de la fecha y hora del escrutinio y del estado **FINALIZADO** del proceso.

8. Datos a completar por la autoridad o el equipo técnico en la diligencia concreta

Campo	Valor
Nombre del proceso participativo	MUNA
Identificador del proceso	770e8400-e29b-41d4-a716-446655440000
Fecha y hora de cierre de la votación	19/07/2026 09:30 a.m.
Fecha y hora del escrutinio	19/07/2026 09:31 a.m.
Total de personas habilitadas	50,684
Total de votantes	50,681
Total de votos válidos	50,681
Total de votos nulos	0
Opción ganadora	Mario Cucinella Architects
Votos del ganador / porcentaje	21,047 - 41.53%
Empate (sí/no)	NO
Hash de integridad del acta	e5abe68a8216020c60a5fa6a9caca482cf93 50b9e1016b592cfd348620ef5918
Autoridad que ejecutó el escrutinio	Ing. Mario David Cantos Salazar

FIRMAS:

ELABORADO POR:	Ing. Anthony Jair Izquierdo Zurita	
FECHA:	19/07/2026	Firma:
ELABORADO POR:	Ing. David Isaac Flores Medrano	
FECHA:	19/07/2026	Firma:
REVISADO POR:	Ing. Oscar Luis Molina Rivera	
FECHA:	19/07/2026	Firma:
APROBADO POR:	Ing. Edwin Wladimir Chica Arteaga	
FECHA:	19/07/2026	