Auditoría sistema de elecciones

Este documento es el resultado del proceso de auditoría realizado al Sistema de Elecciones desarrollado por LACNIC en su versión 2.1.

Para realizar la auditoría se planteó un plan de pruebas con el objetivo de evaluar la funcionalidades que brinda el sistema. El detalle de las pruebas realizadas se encuentra en el Anexo al final del documento.

En primer lugar se evaluaron las funcionalidades realizando pruebas directamente desde la interfaz web. Para las funciones más críticas se realizaron inspecciones de código y en caso de ser necesario pruebas más específicas sobre puntos críticos.

Luego de la ejecución de la pruebas podemos concluir lo siguiente.

Este sistema permite organizar y ejecutar elecciones de forma remota a través de un aplicativo web y la interacción por correo electrónico con los diferentes actores de la misma.

Presenta una interfaz simple y limpia dónde siguiendo la documentación resulta sencillo configurar y llevar a cabo una elección.

En general el sistema se presenta robusto y el flujo de acción de los diferentes actores está restringido a las acciones permitidas y necesarias teniendo así un buen control del uso del sistema no permitiendo alteraciones de resultados por errores o malos usos.

El sistema define dentro de las elecciones roles de contralor (auditor y comisionado) que permiten darle una mayor transparencia al proceso electoral pudiendo ser auditado y en caso de detectarse irregularidades se podrá acceder a los datos crudos de la elección para su análisis.

El sistema brinda la opción de mostrar los candidatos en orden aleatorio dando las mismas condiciones a los candidatos desfavoreciendo sesgos cognitivos.

El sistema presenta una bitácora donde se registran las diferentes acciones que se realizan teniendo un historial detallado de lo que ha ocurrido en el proceso que permite controlar lo sucedido y desalienta malas prácticas.

El sistema debe estar acompañado de un proceso eleccionario (como se plantea en este documento). Realizando pruebas con algunas variantes con mayor complejidad y acciones mal intencionadas encontramos algunos casos que deben tenerse en cuenta al definirlo. De esta manera un proceso adecuado que guíe la correcta ejecución y habilite roles de auditoría sobre el proceso permite llevar adelante una elección transparente con resultados fiables. En estas condiciones de uso el sistema cumple con el objetivo propuesto.

A continuación se presenta el plan de pruebas ejecutado, luego destacamos algunas consideraciones sobre el sistema y planteamos algunas posibles soluciones a futuro.

Plan de pruebas

A continuación se lista una serie de validaciones, categorizadas según su tipo, junto con pruebas que permitan analizar el comportamiento del sistema.

Interfaz web

I. Validaciones en el proceso de votación bajo condiciones normales de uso

A. Votos duplicados

1. Uso de link más de una vez

Descripción	Se intenta votar dos veces consecutivas con un mismo link.
Resultado esperado	Al segundo intento, debe figurar como que ya se votó.
Resultado obtenido	OK.

2. Cancelar selección de candidato y volver a seleccionarlo

Descripción	Seleccionar un candidato, cancelar la selección, seleccionarlo nuevamente.
Resultado esperado	El usuario debería poder votar y su voto quedará registrado una sola vez.
Resultado obtenido	OK.

3. Cancelar selección de un candidato y seleccionar otro

Descripción	Seleccionar un candidato, cancelar la selección, seleccionar un candidato distinto.
Resultado esperado	El usuario debería poder votar y su voto quedará registrado una sola vez (asociado al último candidato seleccionado antes de votar).
Resultado obtenido	OK.

4. Uso de un token modificado:

Descripción	Votar con el token modificado.
Resultado esperado	El usuario no puede votar. El sistema indica que el enlace utilizado no es válido, o un mensaje similar.
Resultado obtenido	OK.

5. Uso de un nuevo token

Descripción	Votar usando el primer link de votación generado. Luego, desde el panel de administrador, generar un nuevo token. Intentar votar nuevamente utilizando el nuevo link de votación.
Resultado esperado	El usuario no puede volver a votar usando el nuevo link, ni usando nuevamente el link anterior.
Resultado obtenido	OK.

6. Seleccionar candidatos de más

Descripción	Seleccionar más candidatos de lo permitido para la elección e intentar confirmar el voto.
Resultado esperado	El sistema indica que el votante debe seleccionar una cantidad menor de candidatos.
Resultado obtenido	OK.

B. Votos perdidos

1. Revisión del panel de auditoría

Descripción	Ejecutar una votación de prueba con al menos 3 votantes y 2 candidatos. Verificar resultados en el panel de auditoría.
Resultado esperado	Los votos se correspondan en número con los votos efectuados.
Resultado obtenido	OK.

2. Revisión del panel de administrador

Descripción	Ejecutar una votación de prueba con al menos 3 votantes y 2 candidatos, habilitando la revisión exhaustiva por parte del administrador. Verificar resultados en el panel de revisión del administrador.
Resultado esperado	Los votos de cada votante se corresponden con los votos efectuados tanto en número como en candidato elegido.
Resultado obtenido	OK.

3. Vencimiento de token

Descripción	Acceder al link de votación y no votar, accediendo nuevamente un tiempo más tarde.
Resultado esperado	El usuario debe seguir habilitado a votar, ya que el link de votación aún está vigente.
Resultado obtenido	OK.

C. Votos fuera del período establecido

1. Votar antes de comenzada la elección

Descripción	Intentar votar antes de la fecha y hora de comienzo de la votación.
Resultado esperado	El usuario no puede votar.
Resultado obtenido	OK.

2. Votar luego de finalizada la elección

Descripción	Intentar votar después de la fecha y hora de fin de la votación.
Resultado esperado	El usuario no puede votar.
Resultado obtenido	OK.

3. Deshabilitar temporalmente los links de votación

Descripción	Deshabilitar los links de votación desde el panel de administrador e intentar votar con el link de un usuario.
Resultado esperado	El usuario no puede votar. El link no caduca y puede ser usado una vez habilitado nuevamente.
Resultado obtenido	OK.

D. Distinto comportamiento dependiendo de la categoría de la elección.

1. Validar que el comportamiento del sistema no depende de la categoría de la elección

Descripción	Repetir las votaciones de prueba anteriores variando la categoría de la votación.
Resultado esperado	Los resultados de cada prueba están de acuerdo a lo esperado en cada caso.
Resultado obtenido	OK.

E. Candidatos mostrados en un orden no aleatorio.

1. Verificación de orden de los candidatos #1

Descripción	Ejecutar una votación de prueba con al menos 2 candidatos, seleccionando la opción de que estos sean mostrados en orden aleatorio. Realizar múltiples votos y verificar en qué orden se muestran los candidatos en cada instancia de voto.
Resultado esperado	Los candidatos se muestran en un orden distinto cada vez que un nuevo usuario va a votar.
Resultado obtenido	OK.
Observación	Cuando el votante tiene EN como su idioma por defecto, el cartel que se muestra al momento de votar es incorrecto: “Candidates are presented in alphabetical order”.

2. Verificación de orden de los candidatos #2

Descripción	Ejecutar una votación de prueba con al menos 2 candidatos, fijando el orden de los mismos. Realizar múltiples votos y verificar en qué orden se muestran los candidatos en cada instancia de voto.
Resultado esperado	Los candidatos se muestran en el orden fijado.
Resultado obtenido	OK.

II. Modificaciones de la elección

A. Votos múltiples

1. Uso de link más de una vez en forma concurrente

Descripción	Se intenta votar dos o más veces de forma concurrente con un mismo link.
Resultado esperado	Al segundo intento, debe figurar como que ya se votó.
Resultado obtenido	OK con excepciones.
Observaciones	Al forzar condiciones de carrera con un breakpoint es posible registrar más de un voto. En condiciones normales no es posible reproducirlo.

B. Cambio de las fechas establecidas de inicio/fin con la votación en curso o ya terminada.

1. Cambiar fecha de inicio de votación en curso

Descripción	Ingresando como administrador principal del sistema, intentar cambiar la fecha de inicio de una votación en curso.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El registro en bitácora indica un cambio en la elección pero no qué cambio se realizó.

2. Cambiar fecha de inicio de votación finalizada

Descripción	Ingresando como administrador principal del sistema, intentar cambiar la fecha de inicio de una votación ya finalizada.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El registro en bitácora indica un cambio en la elección pero no qué cambio se realizó.

3. Cambiar fecha de fin de votación en curso

Descripción	Ingresando como administrador principal del sistema, intentar cambiar la fecha de fin de una votación en curso.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El registro en bitácora indica un cambio en la elección pero no qué cambio se realizó. Al modificar la fecha de fin y deshacer el cambio quedan habilitados los links de auditoría aunque la elección no finalice.

4. Cambiar fecha de fin de votación finalizada

Descripción	Ingresando como administrador principal del sistema, intentar cambiar la fecha de fin de una votación ya finalizada.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El registro en bitácora indica un cambio en la elección pero no qué cambio se realizó. Al modificar la fecha de fin y deshacer el cambio quedan habilitados los links de auditoría aunque la elección no finalice.

C. Edición del padrón de votantes.

1. Editar votante del padrón de una votación en curso

Descripción	Ingresando como administrador principal del sistema, intentar editar la información de un usuario registrado en el padrón de una votación en curso.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El sistema permite la edición de cualquiera de los datos del votante, incluído su email. Si bien en la bitácora queda registrado el hecho, no queda registrado qué campos se modificó ni qué usuario.

2. Editar votante del padrón de una votación ya finalizada

Descripción	Ingresando como administrador principal del sistema, intentar editar la información de un usuario registrado en el padrón de una votación ya finalizada.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El sistema permite la edición de cualquiera de los datos del votante, incluído su email. Si bien en la bitácora queda registrado el hecho, no queda registrado qué campos se modificó ni qué usuario.

3. Eliminar votante del padrón de una votación en curso

Descripción	Ingresando como administrador principal del sistema, intentar eliminar un usuario registrado en el padrón de una votación en curso.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.

4. Eliminar votante del padrón de una votación ya finalizada

Descripción	Ingresando como administrador principal del sistema, intentar eliminar un usuario registrado en el padrón de una votación ya finalizada.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El sistema permite eliminar el votante del padrón, afectando la cifra de votantes habilitados mostrada en el panel de auditoría.

5. Agregar votantes al padrón de una votación en curso

Descripción	Ingresando como administrador principal del sistema, intentar registrar un nuevo votante en el padrón de una votación en curso.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.

6. Agregar votantes al padrón de una votación ya finalizada

Descripción	Ingresando como administrador principal del sistema, intentar registrar un nuevo votante en el padrón de una votación ya finalizada.
Resultado esperado	Queda registrado el cambio en la bitácora.
Resultado obtenido	OK.
Observación	El sistema permite el registro de nuevos votantes, afectando la cifra de votantes habilitados mostrada en el panel de auditoría.

D. Admin puede usar un link de votación directo desde la plataforma o se manda el mail a él mismo.

1. Votar usando el link de un usuario mostrado en la plataforma

Descripción	Ingresando como administrador, entrar al padrón de una votación en curso y visualizar el link de alguno de los votantes que no haya votado. Utilizar el link y registrar un voto.
Resultado esperado	La acción queda registrada en la bitácora.
Resultado obtenido	OK.
Observación	El sistema deja registro de que el link fue visto por el administrador. No se tiene conocimiento si el link fue utilizado y solo el administrador es quien puede consultar toda esta información de la bitácora. Si el link es utilizado el votante recibe el mail de confirmación de voto.

2. Votar usando links de votación recibidos a un mismo mail

Descripción	Ingresando como administrador, entrar al padrón de una votación en curso y realizar la siguiente secuencia de pasos: i. registrar a un nuevo votante con una dirección de correo determinada. ii. utilizar el link de votación enviado al correo del votante registrado para votar en su nombre. iii. editar la información de dicho votante, cambiando su dirección de correo.
Resultado esperado	La acción queda registrada en la bitácora.
Resultado obtenido	OK.
Observación	Es posible, mediante la secuencia de pasos descrita, generar múltiples usuarios que usen una misma dirección de correo para recibir los links de votación. De esta manera, una persona podría recibir en su email múltiples links de votación y votar múltiples veces.

E. Alteración del orden de los candidatos.

1. Fijar posición de uno de los candidatos:

Descripción	Ingresando como administrador, entrar a la configuración de candidatos de una votación con orden aleatorio y modificar el orden de un candidato (usando las flechas provistas para esto) para dejarlo al comienzo o al final de la lista.
Resultado esperado	El sistema indica que hay posiciones fijadas en orden aleatorio.
Resultado obtenido	En el caso de fijar una opción que no corresponda a un candidato en particular no representaría un problema. A la hora de votar se sigue mostrando un cartel que dice “Los candidatos se presentan en un orden aleatorio” por lo que en el caso de un candidato fijado sería bueno informarlo.

F. Eliminación de votos.

1. Eliminar votante que ya votó en una votación en curso:

Descripción	Ingresando como administrador, entrar al padrón de una votación en curso e intentar eliminar del padrón a un votante que ya haya votado.
Resultado esperado	La acción queda registrada en la bitácora.
Resultado obtenido	OK.
Observación	El votante es eliminado del padrón. También es eliminado su voto del sistema.

2. Eliminar votante que ya votó en una votación finalizada:

Descripción	Ingresando como administrador, entrar al padrón de una votación ya finalizada e intentar eliminar del padrón a un votante que ya haya votado.
Resultado esperado	La acción queda registrada en la bitácora.
Resultado obtenido	OK.
Observación	El votante es eliminado del padrón. También es eliminado su voto del sistema.

G. Acceso a funciones de auditor por parte del administrador.

1. Utilizar el link de un auditor desde el panel de administrador:

Descripción	Ingresando como administrador, entrar a la sección de auditores y utilizar el token de auditor como si fuera él.
Resultado esperado	La acción queda registrada en la bitácora.
Resultado obtenido	El administrador puede visualizar el link del auditor, permitiéndole usarlo sin dejar registro de ello en la bitácora.

H. Bitácora incompleta o alterada.

1. Modificar la bitácora:

Descripción	Intentar editar la bitácora. Verificar si todos los administradores y auditores tienen acceso al mismo.
Resultado esperado	La bitácora es inmutable.
Resultado obtenido	OK.
Observación	Si bien la bitácora no puede ser modificada, a través del sistema los datos sólo pueden ser accedidos por el administrador. Es recomendable que en el proceso electoral se dé acceso a esta información a auditores o comisionados.

I. Conocimiento de la distribución de votos antes de terminada la votación.

1. Visualizar resultados parciales siendo administrador:

Descripción	Como administrador, intentar acceder a los resultados de la votación antes de que esta termine.
Resultado esperado	No es posible visualizar los resultados parciales.
Resultado obtenido	OK.
Observación	Existe la posibilidad de modificar la fecha de fin momentáneamente e ingresar a los resultados parciales en ese caso. Queda registro de una actualización en la elección.

2. Visualizar resultados parciales siendo auditor:

Descripción	Repetir la prueba anterior pero entrando con el link de auditor.
Resultado esperado	No es posible visualizar los resultados parciales.
Resultado obtenido	OK.

3. Visualizar resultados parciales siendo votante:

Descripción	Repetir la prueba anterior pero entrando con el link de un votante.
Resultado esperado	No es posible visualizar los resultados parciales.
Resultado obtenido	OK.

J. Asociación de votos a votantes (pérdida de anonimato).

1. Verificar orden de votos en panel de administrador:

Descripción	Como administrador, acceder a los resultados de la votación luego de terminada la misma. Comparar el orden en el que aparecen los votos en la ventana de auditoría con el orden en el que efectivamente se votó.
Resultado esperado	Los votos registrados se muestran en un orden distinto respecto al orden en que fueron ingresados al sistema.
Resultado obtenido	OK.
Observación	El administrador teniendo acceso al link de votación de un votante y teniendo acceso al panel de auditoría tiene la posibilidad de cruzar los datos manualmente.

2. Verificar orden de votos en panel de auditor:

Descripción	Repetir la prueba anterior pero como auditor.
Resultado esperado	Los votos registrados se muestran en un orden distinto respecto al orden en que fueron ingresados al sistema.
Resultado obtenido	OK.

K. Envío de correos de auditoría a direcciones de votantes.

1. Enviar links de auditoría a votantes

Descripción	Como administrador, acceder al menú de envío de correos de una elección en curso e intentar enviar un correo con plantilla para auditores a la dirección de correo de uno o varios votantes.
Resultado esperado	El sistema no permite enviar links de auditoría a personas del padrón.
Resultado obtenido	OK.
Observación	Los correos quedan eternamente como pendientes de enviar.

2. Enviar links de votación a auditores

Descripción	Como administrador, acceder al menú de envío de correos de una elección en curso e intentar enviar un correo con plantilla para auditores a la dirección de correo de uno o varios votantes.
Resultado esperado	El sistema no permite enviar links de auditoría a personas del padrón.
Resultado obtenido	OK.
Observación	Los correos quedan eternamente como pendientes de enviar.

Servicios REST

III. Acceso a recursos protegidos

A. Usar métodos y endpoints diferentes a los definidos

1. Uso de métodos no definidos

Descripción	Intentar acceder a los endpoints de la API utilizando métodos diferentes a GET.
Resultado esperado	La petición es rechazada por el sistema.
Resultado obtenido	OK.

2. Uso de endpoints no definidos

Descripción	Intentar acceder a otros recursos no definidos en la documentación de los servicios.
Resultado esperado	La petición es rechazada por el sistema.
Resultado obtenido	OK.

IV. Acceso a información secreta

A. Acceso a información de votación

1. Identificar a quién votó un votante

Descripción	Analizar la información obtenida de las request GET e intentar identificar a quién votó un votante.
Resultado esperado	No es posible conocer el voto de un votante mediante la información obtenida a través de los endpoints provistos.
Resultado obtenido	OK.

V. Alteración de la votación

A. El consumo de los servicios no altera la votación

1. Consumir cualquiera de los servicios no altera los datos del sistema

Descripción	Realizar una serie de requests a todos los endpoint declarados en la documentación del sistema, intentando para cada una emplear los métodos GET, POST, PUT y DELETE.
Resultado esperado	Ninguna de las request enviadas al sistema provoca un cambio en el estado del mismo.
Resultado obtenido	OK con excepciones.
Observación	Cuando se realiza una request GET a ciertos endpoints correspondientes a la sección de parámetros los datos consultados quedan alterados. Luego de esto el sistema queda inutilizable.

Consideraciones y mejoras propuestas.

Como se menciona en la introducción acompañar el sistema con un proceso que guíe correctamente la elección permite llevar adelante una elección transparente con resultados fiables. A continuación se presentan algunas consideraciones a tener en cuenta en la construcción del proceso acompañadas de mejoras que se podrían implementar para disminuir el impacto de malos usos de la herramienta.

Alteraciones en el padrón.

Durante el transcurso de una elección el administrador puede agregar, modificar y eliminar votantes del padrón. Si bien son funcionalidades que pueden ser útiles en determinadas circunstancias pueden dar lugar a malas prácticas o errores que modifiquen el padrón afectando la elección.

En el caso de una elección finalizada estas funcionalidades no aplican y podrían ser restringidas para ese caso.

La posibilidad de modificar el email de un votante podría dar lugar a otras personas a acceder a votar en su lugar o permitiendo que un mail ya usado para votar pueda volver a usarse nuevamente.

La posibilidad de eliminar votantes puede ser ejecutada aunque el votante ya haya efectuado su voto lo que provoca que su voto también sea eliminado.

Para desalentar este tipo de prácticas se podría indicar en la bitácora cuál usuario y qué campo se modificó. A su vez incluir esta información en el reporte de auditoría permitiría que los auditores chequeen las modificaciones que han sucedido en el transcurso de la elección, a fin de validar que sea una acción que efectivamente tuviera sentido.

Modificar elección.

Es posible modificar la fecha de una elección y sus candidatos. Si bien es una funcionalidad muy útil en determinadas circunstancias luego de comenzada la elección esto puede generar situaciones no controladas como ver resultados parciales o que queden los links de auditoría habilitados mientras transcurre la elección. La posibilidad de quitar candidatos momentáneamente de una elección en transcurso también podría alterar la elección. El registro en bitácora que se realiza de estas actividades desalienta su ejecución, la inclusión de esta información en el reporte de auditoría o el acceso a otras actores encargados del contralor de la elección sería una mejora posible.

Suplantar a votantes y auditores.

Desde la administración del sistema es posible acceder a los enlaces de votación y de auditoría lo que confiere al administrador la posibilidad de suplantar a votantes y auditores.

Para el caso de los votantes el sistema registra en la bitácora el hecho mientras que para los auditores no queda registro. La bitácora es sólo accesible para el administrador por lo que dejar registro en bitácora de estas acciones y disponibilizarlo a los auditores aportaría transparencia.

Por otro lado, teniendo acceso a estos enlaces también permitiría cruzar la información de votos emitidos (link de votación) y resultados (link de auditoría) pudiendo determinar a quién votó un votante en particular.

Aleatoriedad de los candidatos.

En caso de seleccionar la aleatoriedad de los candidatos en una elección los candidatos varían su orden de aparición en la lista. Sin embargo es posible fijar candidatos al inicio o final de la lista restringiendo la aleatoriedad indicada y dejando confuso el término aleatorio en este caso.

Votos duplicados.

Un votante con su link de votación no puede votar más de una vez en condiciones normales. Sin embargo es posible en ciertas condiciones de carrera registrar más de un voto utilizando el enlace de un mismo votante.

Esto se debe a que la sección de código donde se valida que el votante no tenga votos registrados no está mutuoexcluida. Una solución posible es implementar un versionado a nivel de JPA que mutoexcluya la acción de registrar el voto. No importa cuantos votos se intente ingresar solo un proceso podrá grabar el voto.

Servicios que modifican datos.

El sistema cuenta con un conjunto de servicios REST que brindan acceso a la información del sistema cuidando la información sensible del mismo y no permitiendo alteraciones de la información ingresada.

En el caso de los servicios de parámetros se da una condición particular de error al consultar los parámetros protegidos que se devuelven ofuscados (******). En este caso ese valor se termina grabando en la base de datos provocando un resultado que no es el esperado en ese servicio.

Esto se debe a que en el servicio, la entidad *parameter* aún está *managed* cuando se le ofuscan los atributos para ser devuelta. Una posible solución es ejecutar un *detach* antes de ofuscar los parámetros.

Observaciones técnicas

Luego de realizadas las pruebas se detectaron algunos aspectos del sistema que se comentan a continuación.

I. Instalación y configuración

1. Existe un problema de dependencias al instalar el proyecto de forma manual. El paquete javax.annotation no está incluido en el pom del proyecto.
2. En el caso de no tener un servidor de correo con la parametrización por defecto no se indica como realizar la configuración. Se podría mencionar en la documentación el archivo email.properties desde donde se toman configuraciones del servidor de correo en el sistema.
3. Si se modifica el admin se pierde el control del sistema.
4. Los correos equivocados quedan pendientes para siempre.
5. Enlaces erróneos (política de privacidad con enlace a la web de LACNIC, zona de peligro).

II. Funcionamiento

1. Existen endpoints que retornan un código http 200 (OK) al intentar invocarlos con un método distinto de GET, cuando deberían devolver un código 405 (method not allowed).
2. En la vista de bitácora, la fecha es considerada como un string en lugar de un valor de tipo fecha lo que provoca que al ordenar los eventos por fecha no se respete el orden debido. Por ejemplo, un evento ocurrido el 20 de diciembre es considerado como anterior a uno ocurrido el 30 de noviembre.