OEA

Más derechos para más gente

Secretaría para el Fortalecimiento de la Democracia (SFD)

Departamento para la Cooperación y Observación Electoral (DECO)

Auditoría para identificar la o las causas por las cuales no fue posible la correcta implementación del voto automatizado en las elecciones municipales de República Dominicana del 16 de febrero de 2020

INFORME FINAL

Abril de 2020

TABLA DE CONTENIDOS

I. Resumen Ejecutivo

Las elecciones municipales de la República Dominicana estaban planificadas para el día domingo 16 de febrero de 2020. A las 11:11 a.m. de ese día, el Pleno de la Junta Central Electoral (JCE) resolvió suspender la votación, debido a problemas relacionados con el sistema de voto automatizado (voto electrónico) que estaba siendo implementado en 18 distritos electorales y afectaba al 62,04% de los votantes. La falla determinante identificada en el acta 09-2020 del pleno de la Junta Central Electoral consistía en que en un número considerable de las máquinas de voto automatizado no se habían cargado las boletas de manera correcta.[1]

El 21 de febrero de 2020, la JCE solicitó a la Secretaría General de la Organización de los Estados Americanos (OEA), mediante comunicación remitida por la Misión Permanente de la República Dominicana ante la OEA, la conformación de un grupo de expertos para auditar el sistema de voto automatizado implementado en las suspendidas elecciones municipales del pasado 16 de febrero y, de esta manera, identificar la o las causas por las cuales no pudo ser utilizado.

El Secretario General de la OEA, Luis Almagro, aceptó la solicitud de la JCE, coincidente con peticiones del Gobierno nacional y distintos candidatos y partidos políticos, e instruyó al Departamento para la Cooperación y Observación Electoral (DECO) de la Secretaría para el Fortalecimiento de la Democracia (SFD) a realizar los preparativos para llevar adelante una auditoría sobre el proceso de voto automatizado, completa y vinculante en torno a sus resultados, con estándares de calidad técnica y rigor profesional.

El equipo de peritos auditores y expertos electorales designado buscó identificar la o las causas por las cuales no fue posible la correcta implementación del voto automatizado. A continuación, se presenta un resumen sobre los diversos hallazgos de esta auditoría que permiten entender, entre otros asuntos, por qué un gran número de las urnas distribuidas en el país no contaban con la oferta electoral (candidaturas) correctamente instalada.

La causa raíz del problema puede encontrarse en el software diseñado para la personalización de las urnas, es decir, el software utilizado para que cada máquina contara con la oferta electoral y demás datos correspondientes a su mesa. Este software no tenía mecanismos de

[1] Ver Anexo 6.6 - "Acta no. 09-2020 - Acta de la sesión administrativa extraordinaria del pleno de la Junta Central Electoral celebrada el dieciséis (16) de febrero del año dos mil veinte (2020)".

control de integridad[2] de la oferta electoral y, por lo tanto, era incapaz de detectar cualquier tipo de problema que se pudiera haber presentado en el proceso de descarga de las boletas electrónicas. Sumado a lo anterior, la inexistencia de procedimientos formales de prueba del software, impidió que se detectase el defecto durante la fase de "testing" (pruebas).

El equipo de auditoría pudo comprobar la inexistencia de requerimientos formales[3] en el diseño del software lo que facilitó, en consecuencia, este error en el desarrollo del mismo (no controlar la integridad de la oferta electoral). Por tal motivo, se generó un defecto de software, cuya falla se materializó durante la personalización de las urnas.

La Dirección de Informática de la JCE tenía previsto descargar la oferta electoral a cada una de las máquinas en su almacén denominado "La Colina", utilizando para ello una red LAN (Local Area Network). Al descubrir que, con los recursos que contaban hasta el momento, este proceso llevaría más tiempo de lo que tenían planeado y, por tanto, no llegarían a finalizarlo antes de la fecha prevista para el despliegue de las máquinas a los recintos electorales, se decidió utilizar mecanismos de transferencia de la información que no sólo no estaban previstos, sino que tampoco fueron evaluados.

Al uso de la red LAN para viabilizar la personalización de las máquinas, se sumaron módems 3g y 4g que operaban con dos empresas de telecomunicaciones diferentes. Estas herramientas tecnológicas no contaron con un soporte especial por parte de las empresas proveedoras del servicio (debido a que no fue requerido por parte de la JCE). Al intentar descargar archivos de gran tamaño[4] se interrumpió la descarga, quedando la oferta incompleta. En un importante número de urnas no se mostraban todos los candidatos.

Las razones por las que no se detectaron las fallas de manera oportuna se pueden circunscribir a: 1) un software mal diseñado, 2) la falta de testing en las diferentes etapas del proceso y 3) la ausencia de un protocolo de control de calidad. Es decir, no contaban con las herramientas necesarias para identificar y remediar los problemas previo a la distribución de las urnas, por lo que aquellas máquinas con ofertas incompletas llegaron así a los recintos electorales.

[2] Existen numerosos recursos de software para controlar la integridad, que en este caso en particular consistía en validar que la oferta electoral alojada en el servidor se descargara adecuadamente a la urna.
[3] Documento que establece las especificaciones técnicas para el diseño y desarrollo del software.
[4] En el cuerpo del informe se detalla la razón por la cual los archivos eran de gran tamaño.

La falla fue identificada el día sábado previo a la elección y la JCE buscó mitigarla. Sin embargo, tras ensayar dos métodos de mitigación, el día domingo los técnicos intentaron una re-personalización masiva y tuvieron problemas al momento de hacerlo. En algunas ocasiones no sólo no se logró solucionar, sino que al buscar re-personalizar las máquinas en ciertos colegios electorales se descargó la información perteneciente a otro colegio, lo que creó desconcierto entre los técnicos y autoridades en los recintos electorales.

La mañana de la elección, 1.025 colegios, que representaban el 10,50% del total de las urnas, transmitieron el denominado boletín cero con las boletas incompletas. Esta actividad estaba prevista previo al inicio de votación a fin de evidenciar que todas las candidaturas tenían cero votos en la base de datos de la urna.

Un número importante de colegios electorales iniciaron la votación con la oferta electoral incorrecta, asunto que en ese momento ya no podía ser resuelto desde el punto de vista tecnológico.

Del trabajo desarrollado por el equipo técnico que realizó la auditoría se concluye que lo sucedido con la implementación del sistema de votación automatizado fue producto de la mala gestión del área informática de la JCE. El mal diseño del software, sumado a no haber contado con herramientas para detectar o prevenir la falla y no haber podido mitigarla a tiempo, reflejan también la ausencia de protocolos y la falta de aplicación de buenas prácticas. El equipo auditor no encontró evidencia de ataques externos, sabotaje o intento de fraude. Dadas las circunstancias la mañana de la elección, era imposible continuar con la jornada por lo que la suspensión decidida por parte del pleno de la JCE fue correcta.

En este informe, se detallan 21 hallazgos como resultado del proceso de auditoría. A partir de ellos, se especifican las conclusiones de este trabajo y se formulan 10 recomendaciones cuya implementación es esencial para fortalecer el trabajo de la JCE en materia informática y evitar a futuro hechos como los acontecidos en febrero pasado.

II. Introducción

El 21 de febrero de 2020, la Junta Central Electoral (JCE) de la República Dominicana solicitó a la Secretaría General de la Organización de los Estados Americanos (OEA), mediante comunicación remitida por la Misión Permanente la República Dominicana ante la OEA, la conformación de un grupo de expertos para auditar el sistema de voto automatizado implementado en las suspendidas elecciones municipales del pasado 16 de febrero.

El Secretario General de la OEA, Luis Almagro, aceptó la solicitud de la JCE, coincidente con peticiones del Gobierno nacional y distintos candidatos y partidos políticos, e instruyó al Departamento para la Cooperación y Observación Electoral (DECO) de la Secretaría para el Fortalecimiento de la Democracia (SFD) a realizar los preparativos para llevar adelante una auditoría sobre el proceso de voto automatizado, completa y vinculante en torno a sus resultados, con estándares de calidad técnica y rigor profesional.

El 2 de marzo, el Secretario Almagro visitó la República Dominicana, con el objetivo de firmar los dos acuerdos que dieron sustento normativo a este trabajo. Por un lado, el acuerdo suscrito con el Gobierno, representado por Miguel Vargas, Ministro de Relaciones Exteriores, a través del cual se garantizaron los privilegios e inmunidades para que el equipo de expertos internacionales pudiera llevar a cabo su tarea;[5] y, por el otro, el acuerdo de procedimientos para la realización de la auditaría al voto automatizado, firmado con Julio César Castaños, Presidente de la JCE.[6]

[5] Ver Anexo 2.3 – "Enmienda al acuerdo entre la Secretaría General de la Organización de los Estados Americanos y el Gobierno de la República Dominicana relativo a los privilegios e inmunidades de los observadores de las elecciones municipales del 16 de febrero de 2020 y las elecciones presidenciales y congresuales del 17 de mayo de 2020, a efectos de llevar a cabo una auditoría sobre el proceso de voto automatizado implementado en las elecciones municipales del 16 de febrero de 2020."

[6] Ver Anexo 2.4 – "Acuerdo entre la Junta Central Electoral de la República Dominicana y la Secretaría General de la Organización de los Estados Americanos para la realización de una auditoría al proceso de voto automatizado implementado en las elecciones municipales del 16 de febrero de 2020."

III. Antecedentes

Las elecciones municipales de la República Dominicana estaban planificadas para el día domingo 16 de febrero de 2020. A las 11:11 hrs de ese día el Pleno de la JCE, por medio de acta No. 09-2020, aprobó la Resolución que determinó la suspensión de las elecciones generales municipales, debido a problemas relacionados con el sistema de voto automatizado (voto electrónico).

> "*En el caso específico de los 18 municipios donde las elecciones municipales se llevarían a cabo con el sistema de voto automatizado, se ha verificado que, en un número considerable de los equipos no cuantificado, hasta el momento no se cargaron las boletas de manera correcta*".
>
> "*En virtud de lo anterior, este hecho imprevisible ha impedido que en los 18 municipios donde se utilizó el voto automatizado se realicen de manera efectiva las elecciones del nivel municipal, no habiendo la posibilidad real de corregir esta situación en el día de hoy*;" [7]

El 62.04% de la población registrada para votar dependía de este mecanismo para poder cumplir con su derecho constitucional.

A. Marco legal

La Junta Central Electoral es el órgano autónomo que tiene a su cargo la función de organizar, dirigir y supervisar las elecciones. Para ello, cuenta con facultades reglamentarias en los asuntos de su competencia (artículo 212).

En febrero de 2019, el Congreso aprobó la Ley Orgánica del Régimen Electoral 15-19. Entre las diversas disposiciones de esta Ley, se introdujo la posibilidad de que la JCE pudiera establecer la modalidad de voto automatizado de manera progresiva, en consulta con los partidos políticos y debiendo cumplir con un proceso de pruebas con al menos seis meses de anticipación. Así quedó establecido en el artículo 99:

> *"Automatización del Proceso Electoral. La Junta Central Electoral está facultada, en consulta con los partidos políticos, para la automatización progresiva*

[7] Ver Anexo 6.6 – "Acta no. 09-2020 - Acta de la sesión administrativa extraordinaria del pleno de la Junta Central Electoral celebrada el dieciséis (16) de febrero del año dos mil veinte (2020)".

del proceso de votación, ***debiendo probar los sistemas que se usarán, por lo menos con seis (6) meses de anticipación a la fecha de la votación****. Las pruebas podrían incluir simulacros realizados exclusivamente para la validación de los programas y equipos a usar. Los mismos podrán usarse como prueba en las votaciones correspondientes a gremios y organizaciones de la Sociedad Civil."*

El artículo 225 de la misma Ley, otorga a la JCE la facultad para reglamentar el procedimiento de voto electrónico, si se decide emplear este método:

"*Forma de Votar. El votante, ubicado en el lugar indicado, marcará en la o las boletas, previamente firmada(s) y sellada(s) por el presidente del colegio, el o los candidatos de su preferencia, según sea el caso, la doblará y la depositará en la urna correspondiente. En el caso de que se decida la utilización de boletas de tipo electrónico, la Junta Central Electoral reglamentará el procedimiento que se empleará en este sentido. Finalmente, se hará constar en la lista definitiva de electores, que éste ha votado mediante la firma del elector o, en su defecto, con su huella dactilar. Luego se le entintará el dedo índice de la mano izquierda o, a la falta del mismo, otro dedo, en señal de que ya ejerció el sufragio."*

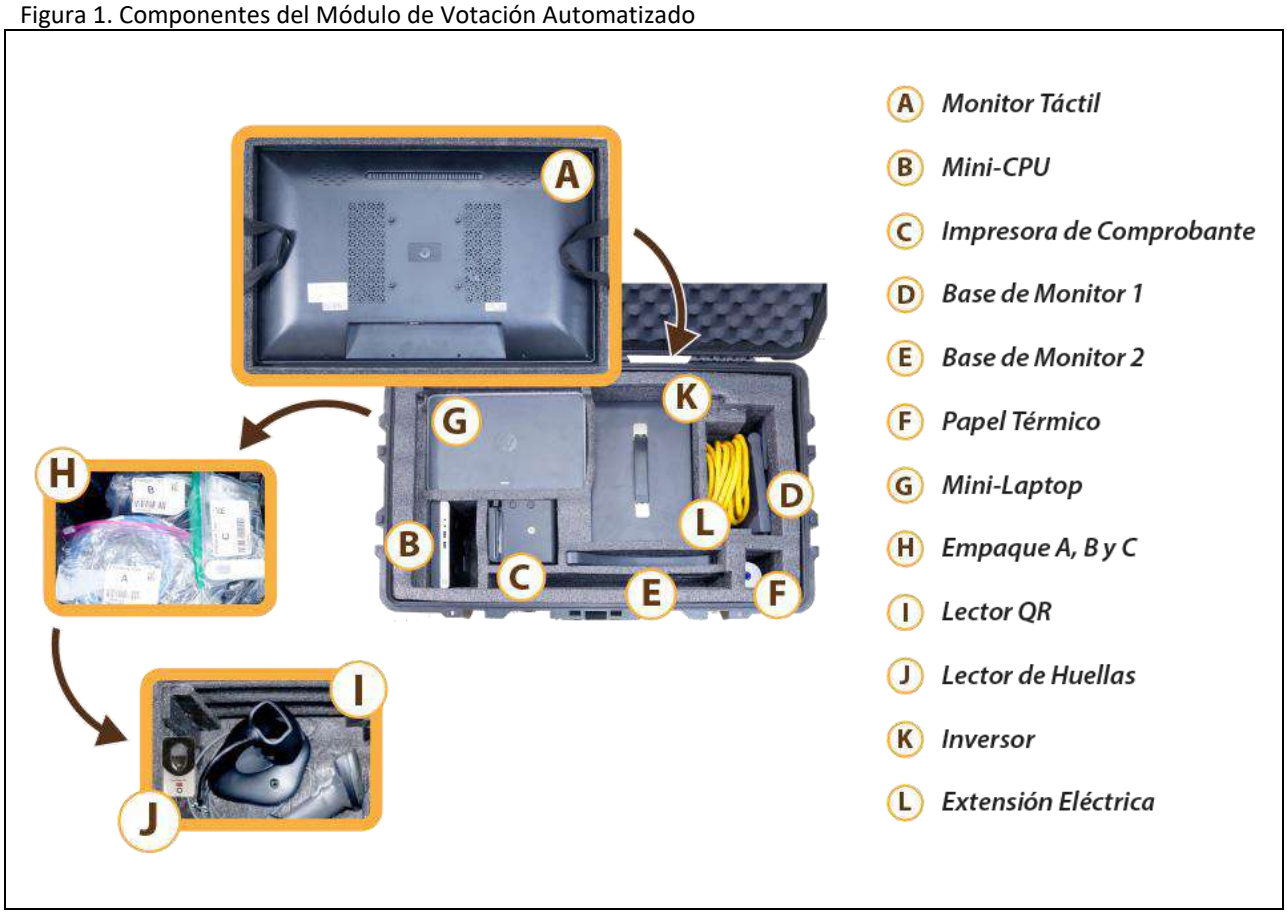
De conformidad con esta disposición, la JCE aprobó disposiciones reglamentarias para establecer votaciones electrónicas en los procesos electorales venideros. El primero de esos procesos correspondió a las elecciones primarias simultáneas del Partido de la Liberación Dominicana (PLD) y del Partido Revolucionario Moderno (PRM) en octubre de 2019[8], con la idea de que después se iniciarían los trabajos preparatorios para las elecciones municipales de febrero de 2020, y las presidenciales y legislativas de mayo del mismo año.

[8] Con la promulgación en 2018 de la Ley 33-18 sobre partidos, agrupaciones y movimientos políticos, los partidos políticos, de acuerdo con el artículo 45, primer párrafo, pueden decidir entre varios mecanismos para la selección de sus candidatas y candidatos, incluidas las elecciones primarias. Cuando se opta por este mecanismo, las primarias deben ser simultáneas entre los partidos que decidan dicho método de selección, y la Junta Central Electoral es el órgano responsable de reglamentar, organizar, administrar, supervisar y arbitrar el proceso de primarias (artículo 46).

B. Módulo y proceso de votación

De acuerdo con el Manual para la Instalación de Módulo de Votación Automatizado[9], desarrollado por la Dirección de Informática de la JCE, el equipo del módulo de votación automatizado estaría conformado por varios componentes (Figura 1).

Figura 1. Componentes del Módulo de Votación Automatizado



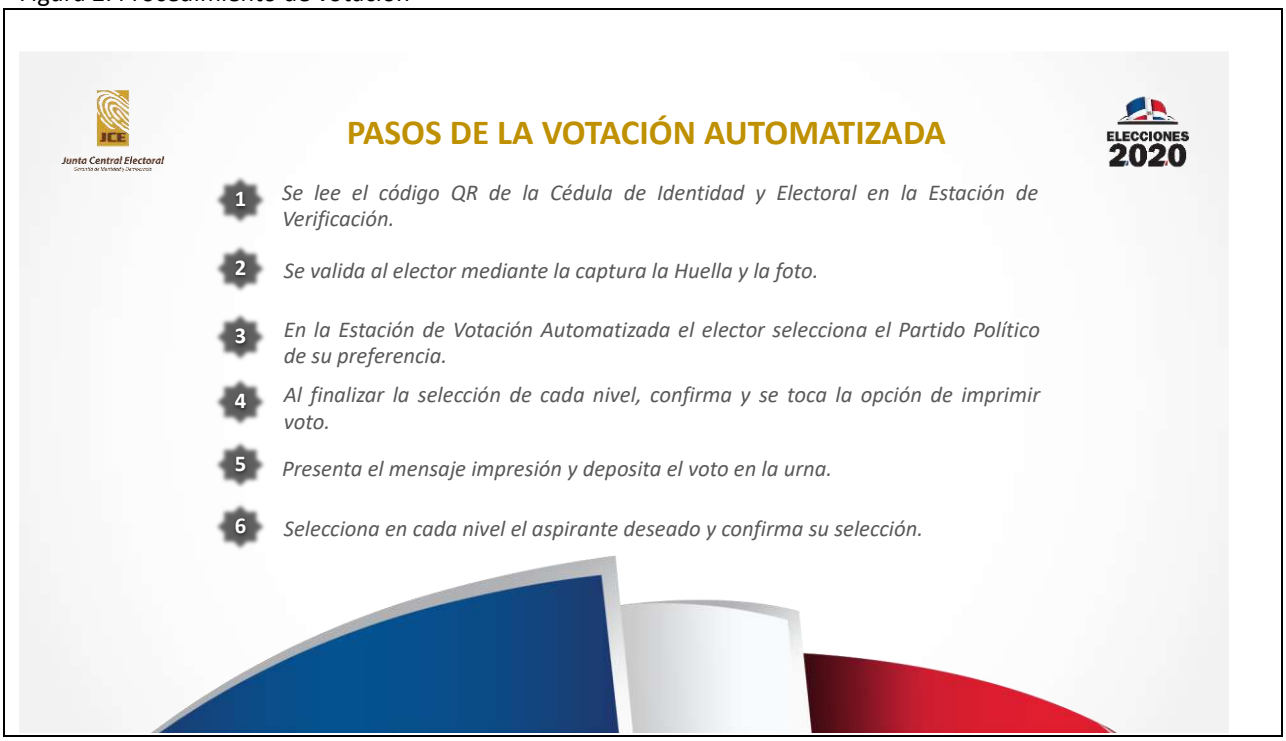
Fuente: Manual de Instalación del Módulo de Votación Automatizado, Dirección de Informática, JCE, 2020.

El procedimiento de votación debía iniciar con la lectura del código QR de la Cédula de Identidad y Electoral de cada ciudadano/a en la estación de Verificación. En la misma estación se debía validar al elector mediante la captura de su huella digital y la verificación de su fotografía.

[9] Ver Anexo 6.1 – "Manual de Instalación del Módulo de Votación Automatizado" Dirección de Informática, JCE, 2020.

Terminado este proceso, el elector debía dirigirse a la Estación de Voto Automatizado, que correspondía a una pantalla táctil. En esta estación o "urna automatizada", el elector seleccionaba los y las candidatas de su preferencia. Al finalizar cada nivel de votación (ofertas en cargos diversos) el elector debía confirmar sus preferencias y seleccionar la opción para imprimir su voto. Hecho lo anterior, se dirigía a la urna, presentaba su mensaje de impresión y depositaba su voto impreso (Figura 2).

Figura 2. Procedimiento de votación



Fuente: Presentación "Sistemas y equipos a utilizar, Elecciones 2020. Elecciones Municipales 16 de febrero de 2020, Dirección de Informática, JCE, 2020"

C. Secuencia de hechos destacados para el informe de auditoría

El 11 de enero de 2020, la Junta Central Electoral aprobó la resolución Res 01/2020[10], mediante la cual determinó los sistemas de votación que serían utilizados en las elecciones del 16 de febrero.

De acuerdo a la resolución, los comicios se celebrarían bajo dos modalidades de votación. Por un lado, se utilizaría el sistema manual (tradicional) en aquellos municipios cuya cantidad de representantes no excediera los 11 regidores. Por el otro, existiría el voto automatizado (electrónico) y conteo manual en las demarcaciones que debían a escoger trece (13) o más regidores, para facilitar la administración y procesamiento de los resultados electorales.

En consecuencia, la votación manual se llevaría a cabo en 140 municipios (del total de 158) y la votación electrónica en el Distrito Nacional y los 17 municipios restantes del país. Estos 17 municipios y el Distrito Nacional concentraban el 62.04% del electorado, distribuido en 9.757 colegios electorales.

Respecto al voto automatizado, la JCE llevó a cabo dos procesos de evaluación externa, principalmente como consecuencia del cuestionamiento de algunos sectores a la gestión de las elecciones primarias de octubre de 2019. En el primero de ellos, realizado por la empresa Alhambra Eidos, se llevó a cabo una auditoría cuyo objeto incluyó verificar el secreto del voto y la no trazabilidad, la integridad de los datos y objetos de la base de datos, el trabajo fuera de linea (no online), el análisis del programa fuente (código fuente) vs programa Objeto de la Unidad de Votación Automatizada y evaluar la infraestructura tecnológica que soporta el Sistema de Votación Automatizada.[11] Entre otros aspectos, se buscó determinar si el software utilizado en las máquinas de votación en aquella oportunidad ejecutaba alguna función o tarea más allá de las necesarias para sus funciones como proveedor de servicio de votación automatizada. [12]

[10] Resolución 01-2020 de la JCE, 11 de enero de 2020. Disponible en: https://jce.gob.do/DesktopModules/Bring2mind/DMX/Download.aspx?EntryId=16167&Command=Core_Download&language=es-ES&PortalId=1&TabId=190

[11] Contrato de prestación de servicios – Auditoría forense al sistema de voto automatizado de la JCE. Disponible en: https://jce.gob.do/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=0&moduleid=416&articleid=2830&documentid=141

[12] Declaración de Alhambra EIDOS sobre Auditoría Forense del Sistema Voto Automatizado de la Junta Central Electoral de la República Dominicana, 31 de enero de 2020. Disponible en: https://jce.gob.do/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=0&moduleid=416&articleid=2890&documentid=166

En segundo lugar, en enero de 2020 la JCE solicitó una evaluación del sistema de voto automatizado a IFES (Fundación Internacional para Sistemas Electorales). Esta no constituyó una auditoría ni tampoco una certificación. La evaluación revisó la funcionalidad del sistema, la capacidad de éste para mantener el anonimato del elector, la auditabilidad del sistema y las funciones de seguridad. También analizó el código fuente y los procedimientos almacenados, así como la capacidad del sistema para capturar con precisión la intención del elector. [13]

Cronología de la Dirección de Informática de la JCE respecto a los hechos del 16 de febrero

Un documento elaborado por la Dirección Nacional de Informática el 18 de febrero de 2020[14] relata la cronología de actividades llevadas a cabo por esa Dirección. Para interés de este informe, se destacan de ese documento tres elementos fundamentales:

1) Una de las tareas críticas realizadas días antes de la elección fue el proceso de clonado y personalización de los equipos a utilizar para la votación electrónica.

Proceso de clonado	Proceso mediante el cual se genera un Sistema Maestro (imagen) con todos los elementos, probados y autorizados por la Dirección de Informática, necesarios para fines de replicar/reproducir exactamente otros equipos. El proceso de clonado inició el 31 de enero 2020 y finalizó el día 3 de febrero 2020.
Proceso de personalización	La personalización es el proceso a través del cual se asigna el colegio electoral al equipo y se cargan los datos de ese colegio que no están precargados en la imagen clonada tales como: fotos de electores, huellas de electores, miembros del colegio y la boleta de candidatos. Para personalizar se debían seguir los siguientes pasos: 1. Tomar uno de los equipos clonados y conectarlo a la red 2. Hacer el test de la unidad para confirmar que podía ser utilizada 3. Pedir autenticación del técnico que la iba a configurar

[13] Informe de la Evaluación Preelectoral del Sistema de Votación Automatizado de la República Dominicana, Fundación Internacional para Sistemas Electorales (IFES), 2020. Disponible en: https://www.ifes.org/sites/default/files/dominican_republic_assessment_report_spanish.pdf

[14] Ver Anexo 6.5 – "Cronología de Actividades Informáticas: Elecciones 16 de febrero 2020", Dirección de Informática, JCE, 18 de febrero de 2020.

	(usuario, clave y huellas) 4. Proceder a la personalización presionando la opción "AUTOMATICA", para que se le asignara al equipo uno de los colegios pendientes de personalizar. a. La opción MANUAL era utilizada para recuperar urnas cuando no tenían comunicación y requerían de un pin adicional, el cual solo era provisto en caso de ser necesario. 5. Validar que el equipo estuviera registrado en el inventario de equipos válidos. 6. Descargar los datos del colegio que no estaban precargados en la imagen clonada: - Fotos de los electores - Huellas de los electores - Miembros del colegio - Boleta de candidatos (los datos se descargaban en orden de partido, candidatos) 7. Validar que las tablas no estuvieran vacías. 8. Imprimir los datos del colegio personalizado para ser colocados en el equipo para fines de identificación.

Fuente: Cronología de Actividades Informáticas. Elecciones 16 de febrero 2020, Dirección de Informática, JCE, 18 de febrero de 2020.

2) El documento da cuenta de las actividades para que los partidos y movimientos políticos pudieran llevar a cabo su registro de alianzas y captura de sus candidatos.

Según la Dirección de Informática, esta actividad inició con entrenamientos al personal técnico en octubre de 2019 y finalizó con la revisión del diseño de boletas y los últimos cambios ordenados por sentencias del Tribunal Superior Electoral (TSE). Este documento señala que hasta el 12 de febrero se habían llevado a cabo 7.486 cambios en candidaturas (y por tanto en boletas) derivado de sentencias del TSE.

De acuerdo a lo que indicó la Dirección de Informática, los "cambios fuera del plazo impactaron sobre los tiempos y la forma de aplicarse otras actividades relativas al clonado de los Kits de votación "CLONADO_FINAL" y a su posterior personalización "PRESONALIZACION_FINAL". Agrega que "más de 7.400 cambios fuera del cierre de la recepción de candidaturas, donde la mayoría se realizaron en fechas posteriores a las

programadas para el inicio de la clonación de los equipos, dieron como consecuencia el cambio en el modelo de Clonado y Personalización de las Urnas".[15]

3) El documento enumera 25 actividades bajo el rubro "Diseño y programación de la urna de votación".

Estas actividades, desarrolladas desde el 4 de enero hasta el día de la elección, consistieron en pruebas de varios tipos, ajustes, simulacros generales, evaluación, validación, entrega del software y claves a los partidos políticos, clonado y personalización final en los equipos, empaque y entrega de los kits de votación a las Juntas Electorales Municipales, así como pruebas de solución de discrepancias.

El documento sostiene que el 3 de febrero no se logró un acuerdo con los partidos políticos para determinar el protocolo de control de calidad de la personalización y el clonado, así como de la verificación del hash y otros elementos de control, debido a las posiciones de algunos partidos. Por ello, según la Dirección de Informática, no se determinó un protocolo.

El sábado 15 de febrero por la tarde, con los kits de votación ya desplegados en los distintos recintos electorales de los municipios con voto automatizado, de acuerdo a la Dirección de Informática *"…algunos kits de votación no contenían la planilla de candidatos completa*".[16]

Por ello, de acuerdo al documento "Cronología de Actividades Informáticas", se diseñó un plan y se inició un operativo pasadas las 4:30 pm para enmendar la situación. Sin embargo, los partidos políticos no estaban al tanto de la situación y solicitaron una reunión con la JCE que se llevó a cabo en horas de la noche previo a los comicios.

Vale mencionar que la Misión de Observación Electoral (MOE) de la OEA, "recibió noticias de problemas con los equipos de votación la noche anterior a las elecciones, ante la denuncia de fuerzas de oposición de que técnicos de la JCE habrían ingresado a los centros de votación a operar los equipos, sin presencia de los delegados de los partidos".[17]

En la reunión que la JCE sostuvo con los partidos, se acordó a las 9:40 pm del sábado la suspensión del operativo para enmendar el problema. Alrededor de la medianoche, resolvieron

[15] Ibíd.
[16] Ibíd.
[17] Informe Preliminar, Misión de Observación Electoral de la Organización de los Estados Americanos, Elecciones Municipales Extraordinarias de la República Dominicana del 15 de marzo de 2020. Disponible en: http://www.oas.org/fpdb/press/Informe-Preliminar-MOE---FINAL.pdf

que sea realizaría entre las 5:00 a.m. y 7:00 a.m. del día de la elección, en presencia de los delegados de los partidos políticos.

Sin embargo, el proceso para enmendar la situación en horas de la mañana del domingo de elecciones no logró corregir los problemas. A la hora contemplada para iniciar la votación, muchos de los equipos de votación (el número exacto no es revelado en el Informe de la Dirección Nacional de Informática) no contaban con la oferta electoral completa.

De acuerdo a lo señalado por la Dirección de Informática de la JCE en la cronología de actividades informáticas,

> "*a las 6.00 am del día 16 de Febrero solo unos 12 colegios habían reportado presencia de los delegados de los partidos y por cuanto eran los únicos que habían iniciado el plan de acción.*
>
> *A las 6.10 am, los delegados de los partidos presentes en la sede central acuerdan con la JCE que el proceso se inicie en los colegios sin la presencia de los delegados del colegio.*
>
> *Al dar inicio al operativo de forma simultánea a menos de 50 minutos de empezar la votación, provocó un pico abrupto de llamadas a la mesa de ayuda que no pudo atender todas las solicitudes a tiempo."*[18]

La MOE/OEA, en su informe preliminar, señaló que durante "las primeras horas de la jornada electoral, la Misión pudo constatar defectos en un alto porcentaje de los equipos instalados (en algunos de los centros de votación observados, hasta el 60% de los equipos presentaron problemas). Los monitores no mostraban la totalidad la oferta electoral". Manifestó también que, sumado al problema identificado en un alto número de colegios, se observó otros como: congelamiento de pantallas, problemas con la impresión del voto y su pliegue para que se mantuviera la secrecía, y dificultades para ingresar el nombre de los delegados.

Agregó que "la capacidad del personal técnico de la JCE se vio rápidamente rebasada, ante la extensión de los fallos y la lentitud de la corrección, que involucraba decisiones centralizadas que aletargaron el proceso". Finalmente, señaló que "los observadores de la OEA desplegados en terreno constataron la imposibilidad de solucionar oportunamente las fallas detectadas y proceder a la votación". [19]

[18] Ibíd.
[19] Ibíd.

A las 11:11 de la mañana, por Resolución del Pleno de la JCE se ordenó suspender las elecciones municipales debido a las razones mencionadas en el acta No. 09-2020 respecto al funcionamiento del sistema de voto automatizado.[20]

[20] Para mayor detalle respecto a la descripción de la Dirección de Informática de la JCE sobre el problema presentado, ver Anexo 6.5 "Cronología de Actividades Informáticas. Elecciones 16 de febrero de 2020".

IV. Auditoría

A. Objetivo de la auditoría

Identificar la o las causas por las cuales no fue posible la correcta implementación del voto automatizado.

B. Equipo Auditor

Para llevar a cabo la auditoría, la Secretaría General de la OEA conformó un equipo de expertos internacionales, que incluyó al coordinador de proyecto del Departamento para la Cooperación y Observación Electoral de la OEA, un perito auditor a cargo del trabajo técnico, un perito auditor responsable de procedimientos y comunicaciones, un perito auditor a cargo de bases de datos y sistema, así como con un consultor de apoyo técnico.

C. Alcance de la auditoría

Conocer a detalle el contexto tecnológico involucrado en el incidente que provocó la mala configuración de las máquinas de voto automatizado, a fin de determinar la causa del problema. Para ello, el equipo auditor realizó un análisis sobre diversos elementos, que incluyó hardware, software, servidores, infraestructura, redes, bases de datos, así como sobre los procedimientos involucrados en su implementación, considerando los procedimientos para la clonación y personalización de equipos, entre otros.

D. Metodología

El equipo de auditoría se instaló en el país el martes 3 de marzo de 2020, y desarrolló labores de campo hasta el martes 17 del mismo mes. Las actividades de auditoría en terreno se planificaron cuidadosamente con la colaboración de los responsables de las áreas competentes de la JCE. Esto permitió minimizar el riesgo de interrupciones en los preparativos de las elecciones municipales extraordinarias que se celebraron el 15 de marzo de 2020.

El equipo auditor realizó un análisis sobre el proceso de voto automatizado utilizado en las elecciones municipales del 16 de febrero, para lo cual procedió a analizar lo siguiente:

I. Documentación

a) Documentación técnica del sistema;
b) Procedimiento de clonado;
c) Procedimiento de personalización de equipos;
d) Manuales del sistema;
e) Guías de usuario;
f) Instructivos;
g) Planes y programas de trabajo;
h) Manuales de soporte técnico;
i) Oferta electoral aprobada;
j) Contrato con empresas de servicios de comunicaciones;
k) Documento denominado cronología de actividades informáticas;
l) Gráficos de mesa de ayuda;
m) Datos exportados de mesa de ayuda;
n) Inventario de equipos de voto automatizado.

II. Componentes

a) Equipos de voto automatizado empleados en la elección en un número que permitió determinar la causa raíz del incidente y sus derivaciones;
b) Equipos de voto automatizado reservados como backup en un número que permitió reproducir la personalización para reproducir la falla;
c) Activos de infraestructura involucrados en el clonado de equipos de voto automatizado;
d) Activos de infraestructura involucrados en la personalización de equipos de voto automatizado;
e) Bases de datos del sistema de votación;
f) Seguridad del sistema en la etapa de personalización;
g) Softwares utilizados para la clonación y personalización.

III. Otros elementos analizados

a) Registros de actividades;
b) Correos electrónicos con antecedentes de interés;
c) Notificaciones de errores y reclamos;
d) Publicaciones sobre la tecnología empleada;
e) Informes previos de auditores y consultores;
f) Antecedentes de la Jornada electoral y del día previo;
g) Estadísticas de equipos que iniciaron votación.

IV. Otras tareas de auditoría

a) Relevamiento del trabajo durante personalización de urnas;
b) Análisis de flujogramas;
c) Visitas a diferentes sitios de almacenamiento;
d) Planificación de entrevistas;
e) Completar listas de verificación;
f) Obtención de muestras;
g) Análisis de informes de seguridad;
h) Análisis de diagramas, logs, antecedentes y configuraciones perimetrales;
i) Análisis de datos.

V. Tareas relacionadas a requerimientos del equipo auditor a la JCE

a) Requerimientos del 001 al 025[21];
b) Seguimiento de los pendientes;
c) Recepción de las entregas;
d) Análisis de la documentación recibida.

VI. Entrevistas concretadas

a) Dirección Nacional de Elecciones;
b) Subdirector Nacional de Elecciones;
c) Director de Informática;

[21] Ver Anexo 3.1 – Requerimientos de Información a la Junta Central Electoral.

d) Subdirector de Informática - Responsable de Base de Datos;
e) Subdirector de Informática - Desarrollo de Sistemas;
f) Subdirector de Informática - Redes e Infraestructuras;
g) Subdirector de Informática - Administración y Logística;
h) Desarrollador de Sistemas/Programador;
i) Desarrollador de Aplicaciones;
j) Responsables de Help Desk;
k) Responsable de Testing;
l) Encargado de Soporte al Usuario;
m) Encargado de Documentación, Pruebas y Entrenamientos;
n) Encargado de Soporte Técnico;
o) Encargado de Comunicaciones y Redes;
p) Encargado de Sala de Máquinas;
q) Administrador de Base de Datos;
r) Responsable de seguridad de equipos de Voto Automatizado;
s) Asesor Externo de Seguridad Informática;
t) Responsables de Publicación de Resultados.

VII. Preservación

Se llevaron adelante copias del contenido de los discos rígidos de un conjunto de equipos de voto automatizado (Mini Pc). Esto se realizó a fin de conservar dos ejemplares de la copia del disco por cada situación diferente que se presentó (oferta: correcta, incorrecta, corregida y mal mitigada). Para realizar estas copias, se empleó un procedimiento de copia forense, efectuando una copia denominada “bit a bit”.

Las copias se realizaron para preservar el estado de dichos equipos en poder de los auditores, a pesar de que el análisis realizado no afectaba a los equipos y solo se extrajo información para análisis en laboratorio.

Los logs (registros) de equipos auditados se preservan en poder del equipo auditor como evidencia de auditoría.

El conjunto de equipos analizados se entregó precintado y en perfecto estado. La JCE puede analizar los equipos que ya fueron devueltos al almacén.

VIII. Selección de equipos y análisis en laboratorio

Para comenzar las tareas de auditoría, se seleccionó un grupo inicial de 60 máquinas de voto automatizado utilizadas durante las suspendidas elecciones municipales, que habían protagonizado las diferentes situaciones planteadas durante el incidente. A estas se sumaron 20 máquinas que habían estado dispuestas como backup.

Los equipos de backup fueron analizados para posteriormente emplearlos en la reconstrucción de la falla. De este modo, se realizaron pruebas sin afectar los equipos ya personalizados.

Con el avance de las investigaciones, el equipo auditor sumó a su análisis un lote de 75 máquinas que habían sido utilizadas en diversos municipios. Esta muestra correspondió a equipos en los que se había intentado mitigar la oferta electoral de forma infructuosa (al menos en una ocasión).

Posteriormente se sumó al estudio 179 equipos, seleccionados aleatoriamente por personal ajeno al equipo auditor y a la JCE, que se hallaba prestando servicios de guardia en el almacén.

Finalmente, se solicitó al personal de almacén seleccionar aleatoriamente contenedores para analizar los últimos 200 equipos. Lo hicieron de manera independiente, escogiendo y apartando contenedores del almacén.

En total, fueron analizados 534 equipos de voto automatizado. En el Anexo I “Análisis de equipos de voto automatizado” se puede observar un resumen de los resultados de los análisis efectuados respecto a la oferta electoral.

IX. Apoyo de personal técnico de la JCE al servicio de equipo auditor

Para lograr cumplir con el plan de auditoría, se requirió la presencia de un técnico y un ayudante de la JCE para facilitar los desplazamientos y montaje de equipos en el laboratorio donde trabajó el equipo de auditoría.

Luego de algunas demoras, la JCE asignó dos personas como ayudantes y un técnico permanente. Personal adicional del área de logística prestó colaboración para los últimos traslados de equipos. Ellos mismos regresaron al depósito los equipos una vez analizados y debidamente precintados.

X. Pruebas con especialistas de la JCE

Se llevaron adelante numerosas pruebas en diferentes escenarios, para recrear el proceso de descarga de la oferta electoral. Se personalizaron equipos de backup mediante módems 3g y módems 4g, logrando con esta última tecnología (4g) reproducir la falla en cada una de las pruebas. Por cada prueba se realizaron varios intentos de descarga de la oferta electoral y, en promedio, se detectaron fallas en más del 51% de estos intentos, ocasiones en las que se descargó parcialmente la boleta.

Se sistematizaron las pruebas junto a subdirectores de la JCE, quienes tienen en su poder los scripts, datos de entrada, logs, otras evidencias y el resultado de cada intento. Para demostrar que la falla con los modems 4g no estaba relacionada con la urna, sino que se trataba de interrupciones en la comunicación, se realizó una prueba descargando el archivo con la oferta electoral desde el servidor a una notebook. En dicha prueba, sobre un total de once intentos totales realizados, la oferta electoral se descargó incompleta en seis oportunidades.

Se efectuaron además capturas de tráfico de datos durante las pruebas para contar con elementos de análisis más específicos. Las mismas se encuentran en poder del responsable de redes e infraestructuras de la JCE y una copia la conserva el equipo auditor.

V. Hallazgos

1. Falta de estandarización de las imágenes de candidatos para voto automatizado

La JCE no estableció un criterio estandarizado para que los partidos políticos proveyeran las imágenes de candidatas y candidatos a ser incorporados en las diversas ofertas electorales. En consecuencia, se recibieron imágenes que en algunos casos fueron de gran tamaño (peso en bytes). Los técnicos de la JCE tampoco redujeron el tamaño de esas imágenes a la hora de incorporarlas al sistema.

Esto ocasionó que el grupo de imágenes correspondiente a la oferta electoral, que debía incorporarse a la base de datos de cada urna durante la personalización, fuese de gran tamaño, lo que constituyó un factor para la interrupción de la descarga de la oferta durante la personalización.

2. Falta de control de integridad en el software de personalización de las urnas

El software diseñado para la personalización de la urna no incluyó el control de integridad de la oferta electoral que se descargaba en un archivo.

Existen numerosos recursos de software para controlar la integridad que, en este caso en particular, consistía en validar que la oferta electoral alojada en el servidor se descargara adecuadamente a la urna. Era suficiente con seleccionar uno de los recursos disponibles y aplicarlo en el proceso de personalización.

No contar con esta medida esencial de control fue lo que facilitó la materialización de la falla. En caso de haber existido, los técnicos habrían podido detectar que no se había descargado la totalidad de la información desde el servidor a la urna y habrían alertado para que no se tomara como válida dicha personalización.

La falla consistió en la descarga incompleta de la oferta electoral incorporada a la urna, es decir, sin contar con la totalidad de los candidatos.

3. El proceso de personalización no mostró mensajes alertando de la falla

a) Si bien el proceso contemplaba dos opciones de personalización (manual y automática), se configuró para ejecutarlo en forma automática, por lo que el usuario solo esperaba a que concluyera el procedimiento.

b) Los funcionarios de la JCE que llevaron adelante la tarea no eran expertos, sino simples usuarios del sistema, y no recibieron alertas del software sobre fallas en la descarga de la oferta electoral.

c) La utilidad BCP (Bulk Copy Program), es una línea de comando con la cual se programa la copia masiva de datos entre una instancia de SQL Server y un archivo de datos (utilizando un archivo de formato especial). Este comando se utilizó en el procedimiento de personalización de las urnas y tal como fue configurado, no reportó error alguno durante el proceso (independientemente de la red empleada para personalizar la urna).

4. No se analizó previamente la infraestructura de redes antes de personalizar las urnas

La personalización de las urnas se inició utilizando la red LAN instalada en el almacén denominado “La Colina”, perteneciente a la JCE. Esta red LAN no fue evaluada para saber si podría soportar la carga de trabajo (con una oferta electoral de gran tamaño en bytes) para la personalización de forma simultánea de las urnas.

Por la saturación del enlace de red entre “La Colina” y la sede central de la JCE, el proceso de personalización se tornó lento, al punto de comprometer los plazos previstos para el despliegue del kit tecnológico para la jornada electoral.

En virtud de esta lentitud y apremiados por el tiempo, los técnicos de la JCE optaron por otras alternativas para complementar los puestos que personalizaban urnas mediante la red LAN. Particularmente, se analizó habilitar la personalización mediante enlace inalámbrico utilizando módems USB 3g y 4g.

En ningún caso se analizó el impacto del empleo de numerosos puestos (conexiones a la red) que de manera concurrente generaban tráfico al descargar una oferta electoral de gran tamaño (peso en bytes). Esto pudo haber ocasionado problemas adicionales de red e interrupciones de procesos, que no fueron contemplados y que pudieron haber propiciado la materialización de la falla de oferta incompleta.

Otro aspecto relevante es que no se analizó el conjunto de protocolos de red a emplear, como el Tabular Data Stream (TDS) y su comportamiento con los volúmenes, la tecnología, las limitaciones de la red y los servicios existentes.

Arquitectura planificada – Flujo Personalización de equipos del Voto Automatizado

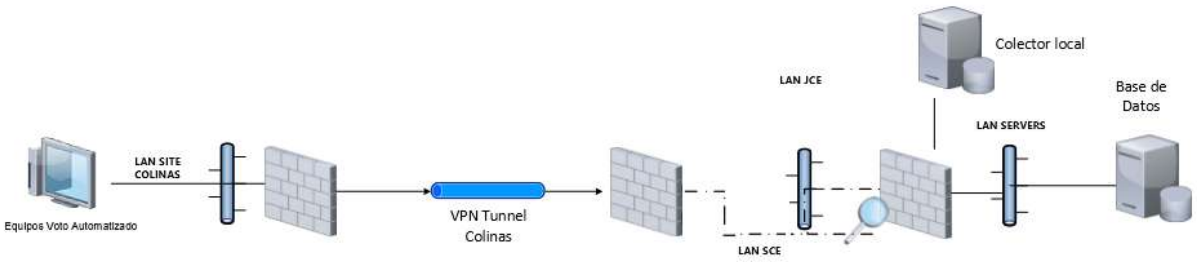


Diagrama adaptado por equipo auditor OEA

5. **El área de redes propuso incorporar módems 3G para la personalización de urnas, sin realizar un análisis previo de su capacidad para transmitir el volumen de datos necesario para la personalización de las urnas**

Se dispuso un pequeño grupo de módems 3G (seis aproximadamente), que aportó puestos complementarios a los de la red LAN que estaban en uso. Estos dispositivos inalámbricos resultaron insuficientes finalmente.

Al emplear estos módems, se produjo un incidente de seguridad de la información, ya que se afectó la integridad de la oferta electoral dado que se descargó incompleta en un grupo de urnas.

El área de seguridad informática de la JCE no detectó este problema y, por lo tanto, tampoco calificó este incidente de seguridad de la información. Por la misma razón, no realizó reclamos oportunos a la empresa proveedora.

El equipo auditor realizó diferentes pruebas de forma independiente y en conjunto con los técnicos de la JCE sin lograr reproducir la falla con los módems 3G.

Arquitectura incorporando 3g – Flujo Personalización de equipos del Voto Automatizado

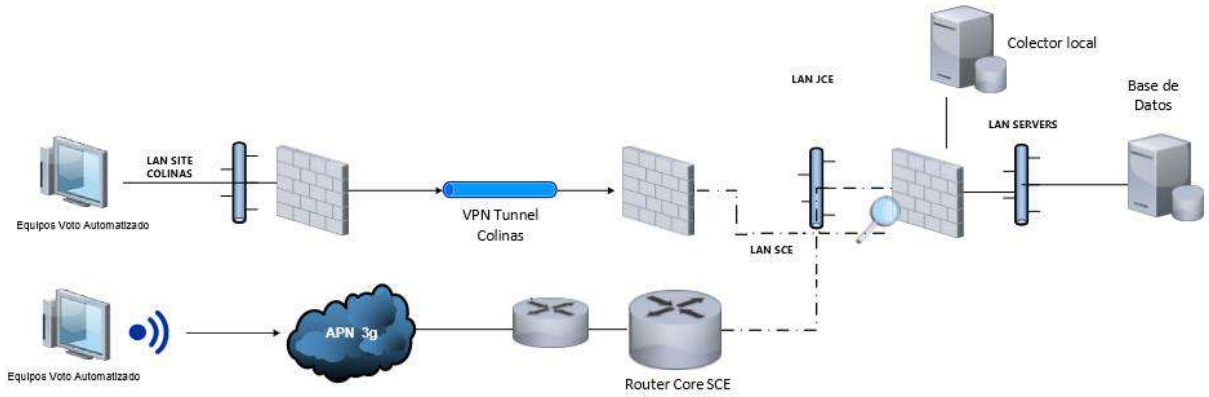


Diagrama adaptado por equipo auditor OEA

6. **El área de redes propuso emplear módems 4g, justificando la decisión en la velocidad que podría aportar esta tecnología**

Se inició la personalización mediante esta red con aproximadamente seis módems. Al percibir una velocidad que superaba las expectativas (sin notar que se interrumpía la descarga y por eso culminaba rápidamente el proceso), se procedió a disponer una cantidad cercana a los treinta módems 4g pese a que:

a) No se había evaluado esta tecnología para la personalización, con una demanda como la que impondría la oferta electoral debido a imágenes no estandarizadas y, en algunos casos, de gran tamaño en bytes;

b) Tampoco se comunicó a la compañía proveedora que se requería un ancho de banda y prestaciones de servicio especiales para llevar adelante la personalización de urnas, lo que hubiese permitido contar con las previsiones del caso por parte de su personal de soporte técnico;

c) El contrato con la compañía proveedora de módems 4g no contaba con Acuerdo de Nivel de Servicio o SLA por sus siglas en inglés (Service Level Agreement) que garantizase el desempeño esperado en este tipo de tareas (que no son comunes, por el peso en bytes de las imágenes y la criticidad del proceso);

d) No se solicitó soporte especial a la compañía proveedora de módems 4g para asistir a la JCE durante la personalización de urnas, lo que pudo haber permitido contar con prestaciones de servicio especiales y, tal vez, la posibilidad de detectar el error oportunamente mediante análisis de tráfico y comprobación de interrupciones.

En un número importante de oportunidades el proceso de descarga de la oferta electoral se interrumpía con esta tecnología. Es decir, se produjo también un incidente de seguridad de la información, ya que afectó la integridad de la oferta electoral en un gran número de urnas.

Al igual que en el caso descrito en el hallazgo 5, el área responsable de la seguridad de la información de la JCE no detectó y, por lo tanto, no calificó este incidente de seguridad de la información. Por la misma razón, tampoco realizó reclamos oportunos a la empresa proveedora.

Debido a la cantidad de módems 4g que se habilitaron y a las interrupciones que se produjeron en las comunicaciones, el impacto de las fallas con esta tecnología afectó a un gran número de urnas.

El equipo auditor pudo reproducir la falla en diferentes pruebas efectuadas en forma independiente, al igual que en las llevadas adelante con los técnicos de la JCE y las realizadas en presencia de funcionarios de la empresa proveedora de módems 4g, el día 10 de marzo de 2020.

Un antecedente que se debe tener en cuenta, y que fue documentado por el equipo auditor, está vinculado al proceso de personalización de las urnas implementado para las elecciones primarias. En esa oportunidad, el área de testing realizó las pruebas correspondientes y detectó una falla en el uso de los módems USB en esta APN (Access Point Name). Ello permitió advertir a tiempo a la empresa proveedora, que determinó que resultaba insuficiente el ancho de banda del equipo terminal de su APN colocado en la sede de la JCE y procedió a resolver el problema. Esta falla fue mitigada a tiempo y, por tanto, no tuvo impacto alguno en la integridad y disponibilidad de la información.

Para las elecciones municipales, el área de testing no fue informada respecto a la utilización de los módems USB, por lo que no realizó las pruebas que correspondían. Sin embargo, este antecedente debió servir de alerta para que se analizara la infraestructura, se consultara con la empresa proveedora y se solicitara un servicio de soporte especial por parte de la contratista. Sobre todo, si se tiene en cuenta que el proceso de las elecciones municipales requería una capacidad de ancho de banda muy superior a la de las elecciones primarias.

Arquitectura incorporando 4g – Flujo Personalización de equipos del Voto Automatizado

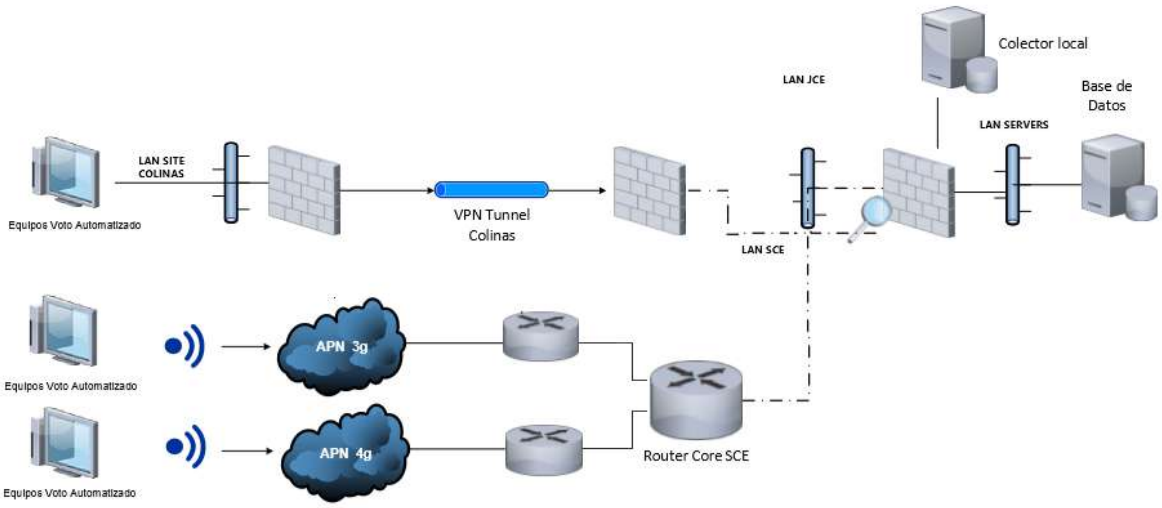


Diagrama adaptado por equipo auditor OEA

7. Ausencia de un protocolo para el control de calidad del clonado y la personalización

Esta situación es clave en la cadena de sucesos que favorecieron el despliegue de equipos con la oferta electoral incompleta. Se trata de una grave deficiencia en el control, que debió llevarse adelante sin depender de terceros. El personal técnico de la JCE justificó su ausencia debido a lo siguiente:

- Existió una convocatoria a los partidos políticos para determinar en conjunto con ellos el protocolo para el control de calidad de la personalización y el clonado, que incluyese la verificación del hash[22] (entre otros elementos de control).
- Según la Dirección de Informática, la reunión terminó sin ningún acuerdo sobre el protocolo de control de calidad de la personalización, debido a las posiciones de algunos partidos. Los partidos solicitaron hacer el control el día de la instalación de los equipos, y que se le entregara la lista de los seriales de todas las urnas automatizadas.
- Al no haber acuerdo, no se definió el protocolo para control de calidad y validación de la personalización de los Kits de Votación.

8. La mitigación (o resolución) de la falla no estaba planificada y resultó deficiente

En caso de que hubiera algún problema, la única medida de contingencia contemplada era el reemplazo de máquinas. Por lo tanto, inicialmente se procuró la sustitución de equipos, hasta comprobar que la cantidad de equipos de backup no era suficiente para solucionar el problema.

Se buscó entonces remediar la falla mediante una re-personalización controlada. En este caso, dos expertos guiaban al técnico para lograr la corrección.

Se procedió a reducir el tamaño de las imágenes correspondientes a la oferta electoral a ser descargada, debido a que notaban la demora por el peso en bytes de las imágenes.

Se decidió finalmente aplicar, como método de mitigación, la re-personalización no asistida por expertos a fin de hacerlo masivamente ante el número de equipos detectados con la oferta electoral incorrecta.

[22] Una función criptográfica hash, es un algoritmo matemático que transforma cualquier bloque arbitrario de datos (por ejemplo el contenido de un archivo de datos) en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud, que depende del algoritmo usado.

9. **Se produjo entonces un nuevo y grave incidente de seguridad de la información, ya que ciertas mesas se re-personalizaron con la información de otra, lo que afectó la integridad y la disponibilidad de la información**

Numerosas mesas fueron re-personalizadas con la información de otra mesa, lo que constituyó una falla de alto impacto ya que no se podía iniciar votación en esas condiciones.

El equipo auditor analizó 75 equipos de este universo y constató la descarga de más de una oferta en cada una de ellas.

Una urna que se personalizó erróneamente con datos de otra mesa (como ejemplo) – Tomada por equipo auditor

Una de las urnas analizada por los auditores, que presentaba esta falla, marcaba la hora de re-personalización a las 10:50 del domingo 16 de febrero de 2020. Este dato muestra que, a escasos minutos de la suspensión de las elecciones, se continuaba re-personalizando de manera incorrecta.

A requerimiento del equipo auditor, el equipo técnico de la JCE documentó cómo se efectuó el proceso de corrección de la oferta electoral y su diagnóstico de la nueva falla que comprometió la remediación. (Anexo 5 – Procedimiento de remediación JCE)

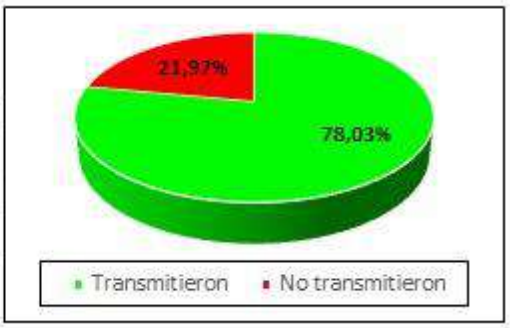
10. Un importante grupo de urnas no transmitió boletín cero

Previo al inicio de la votación, las urnas debían transmitir el denominado boletín cero, un resumen para demostrar que todas las candidaturas tenían cero votos en la base de datos de la urna. En caso de que el proceso hubiera sido exitoso, se debió haber conectado y transmitido el 100% de los equipos, es decir, 9.757 unidades.

Se comprobó que solo transmitieron 7.613 urnas, por lo que quedaron sin transmitir el boletín cero 2.144 urnas.

MESAS QUE TRANSMITIERON BOLETÍN CERO

SITUACIÓN	CANTIDAD
Transmitieron	7613
No transmitieron	2144
TOTAL	**9757**



11. Inicio de la votación con oferta incorrecta

Conforme a lo descrito en diversos hallazgos, un número importante de colegios electorales iniciaron la votación con la oferta electoral incorrecta, situación inaceptable en un proceso electoral.

Si bien no es posible determinar exactamente el número que inició en esas condiciones, se pudo determinar que 1.025 urnas (10,50% del total) transmitieron el boletín cero con la oferta incompleta. Dado que la transmisión del boletín cero es la tarea previa al inicio de votación, este porcentaje de urnas es representativo.

MESAS QUE TRANSMITIERON BOLETÍN CERO CON OFERTA ELECTORAL INCORRECTA
(sin mitigar)

SITUACIÓN	CANTIDAD
Transmitieron sin mitigar	1025
Resto de las mesas	8732
TOTAL	**9757**

De no haberse suspendido la elección, las mesas que iniciaron la votación en tal circunstancia habrían sido anuladas con posterioridad por ofrecer una oferta electoral incompleta al elector.

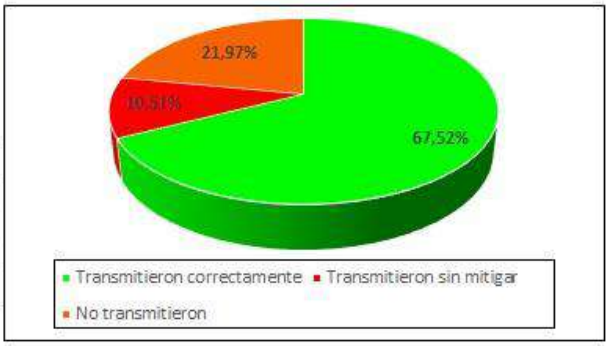
Esta grave situación pone en evidencia falencias de coordinación en el operativo de mitigación de la falla y deficiente comunicación.

12. Solo un porcentaje de urnas estuvo en condiciones de ser utilizada para la votación

Si se consideran las urnas que transmitieron el boletín cero (con la oferta correcta), se puede establecer que solo un porcentaje del total esperado logró estar en condiciones de iniciar votación. Estos datos se extrajeron de la base de datos de la JCE, que guarda en un campo si cumplió con la transmisión. No da certeza que se haya iniciado la votación con esa urna.

MESAS QUE TRANSMITIERON BOLETIN CERO CON OFERTA ELECTORAL CORRECTA
(En condiciones de iniciar votación)

SITUACIÓN	CANTIDAD
Transmitieron correctamente	6588
Transmitieron sin mitigar	1025
No transmitieron	2144
TOTAL	**9757**



13. Al momento del repliegue, no se estableció una cadena de custodia como recomiendan las buenas prácticas

El equipo de auditoría detectó que al momento del repliegue no se realizó una preservación adecuada de los equipos. Por ejemplo, escasas maletas iniciaron el repliegue con precintos, numerosos kits no contaban con la memoria flash de back up y algunos kits contenían varias memorias flash en su interior.

Sin embargo, ya en el almacén "La Colina", estuvieron debidamente custodiadas y contaron con un servicio de vigilancia mediante cámaras.

14. Mesa de ayuda y soporte no planificada para un proyecto de tamaña envergadura.

El personal técnico de la JCE contempló una cantidad limitada de situaciones que se podían presentar. No previeron situaciones críticas que pudieran escalarse a un nivel especializado y en el volumen en que se dieron, debido a la cantidad de urnas con la oferta incorrecta. Se puede observar en el informe de incidentes[23] que se presentaron de manera concurrente llamadas por otros conceptos, lo que hizo colapsar el servicio.

La mesa de ayuda solo registró 2.676 boletas incorrectas cuando la cantidad era muy superior. Además, no registró, con un concepto identificable, la descarga de la información de una mesa incorrecta sobre la solicitada al intentar re-personalizar (por la falla en la mitigación). Esto debió haber quedado registrado por ser un incidente de seguridad que afectó tanto a la integridad como a la disponibilidad de la información.

No hubo un plan de contingencias y, por ende, faltó un plan de acción de emergencia.

Se perdió el control de la mesa de ayuda, lo que generó que los propios responsables del sistema debieran atender las llamadas e incidentes y, en consecuencia, les imposibilitó analizar la casuística y brindar soluciones al escenario de caos que existió.

[23] Ver Anexo 4.5 – "Informe de incidentes de mesa de ayuda".

Debió reiniciarse el sistema que soportaba la mesa de ayuda en más de una ocasión y las demoras en la atención fueron cada vez más frecuente durante la mañana del domingo de elecciones.

15. Información no estandarizada e inconsistente

En el recinto de mesa de ayuda, se proyectaba la siguiente información relativa al voto automatizado, en un reporte que se titulaba *Inicio de Votación – Modalidad Automatizada*:

- Total de colegios;
- Colegios que han iniciado votación;
- Colegios que no han iniciado votación;
- Gráfico de inicio de votación por hora;
- Porcentaje de inicio de votación.

Durante la mañana del domingo, diferentes grupos de observadores internacionales estuvieron consultando la información de dichas pantallas. A medida que avanzó la mañana y ante la falta de información brindada por el área informática, representantes de las agrupaciones políticas se hicieron presentes en este recinto. Tuvieron acceso a la información de las pantallas hasta que fueron convocados a una reunión (previa a la suspensión de las elecciones).

Respecto a la información desplegada del voto automatizado en esas pantallas, el equipo auditor pudo validar lo siguiente:

- El número de colegios electorales que habían iniciado votación era incorrecto;
- El número de colegios electorales que no habían iniciado votación era inexacto;
- La información no se actualizaba con cada inicio de votación en los recintos;
- El responsable de testing no llevó adelante pruebas sobre este aplicativo;
- Aun cuando el objetivo primario del diseño no fuese la divulgación a terceros, la información era inexacta para quien la consultase.

16. Se carece de datos vitales para las estadísticas y análisis

Ante lo sucedido, era razonable recurrir a una serie de datos que permitieran preparar información estadística y practicar análisis detallados. Sin embargo, esto no fue posible debido a que no se cuenta con los siguientes datos:

a) Red empleada para la personalización de cada urna de forma indubitable. Solo se cuenta con información parcial que permite señalar un porcentaje de urnas como personalizadas por una red determinada en los casos en que un técnico haya utilizado únicamente una red para personalizar.

b) Cantidad de fallas por cada red utilizada (por lo descripto en el ítem a);

c) Número exacto de colegios electorales que iniciaron votación (solo se conocen los que transmitieron boletín cero con boletas correctas);

d) Colegios electorales que iniciaron la votación con la oferta incorrecta (solo se sabe los que transmitieron boletín cero con boletas incompletas).

17. La documentación técnica del software es escasa

Se pudo relevar que se retomó un desarrollo de software que había sido discontinuado y no contaba con requerimientos de software ni documentación formal.

No existen casos de uso[24] del voto automatizado. Si bien se inició el desarrollo de los mismos, las tareas fueron interrumpidas.

18. No se cuenta con un proceso formal de desarrollo de software

Si bien el personal que desarrolla es experimentado y calificado, no cuenta con un procedimiento formal para el desarrollo, las pruebas ni la liberación del software.

[24] Un caso de uso es la descripción de una acción o actividad. Un diagrama de caso de uso es una descripción de las actividades que deberá realizar alguien o algo para llevar a cabo algún proceso. Los personajes o entidades que participarán en un diagrama de caso de uso se denominan actores.

19. No se preservaron todos los artefactos de software[25] e ítems de configuración involucrados en el proceso

Mediante el proceso de preservación del software (o congelamiento), solo se preservó parte del software. Este procedimiento se centró en la máquina de votación.

Particularmente, los artefactos involucrados en la auditoría y causa raíz del incidente de seguridad inicial, no estaban preservados.

20. El área de testeo no hizo pruebas (testing) formales de software

El equipo de auditoría pudo comprobar deficiencias en materia de testing:

a) Solo se practicó test de caja negra[26] (parcialmente);

b) No se contó con casos de prueba formales;

c) No se realizó testing unitario del software, una de las formas de garantizar la eficiencia del mismo. Combinado con la inspección de software (que tampoco se aplicó), aportan el grado de revisión esperado;

d) No se contó con testing unitario y automatización de los casos de testing para todo el código;

e) No se realizó un test de regresión controlado por la JCE que pudiera verificar que una refactorización no afectara los demás artefactos que habían sido probados previamente. Esto representó un riesgo adicional al aplicar modificaciones de software.

[25] Artefacto de software: Cualquier elemento que resulte del proceso de desarrollo de software, por ejemplo, documentos de requisitos, especificaciones, diseños, modelos, descripciones, software, etc.

[26] El test de caja negra es una técnica de pruebas de software en la cual la funcionalidad se verifica sin tomar en cuenta la estructura interna del artefacto, detalles de implementación o escenarios de ejecución internos en el software.

21. No se contó con un proceso formal de identificación de defectos de software y su gestión.

No existe un procedimiento de identificación de defectos.
No se halló un procedimiento para el seguimiento del ciclo de vida de los defectos.

VI. Conclusiones

1. La ejecución de un proceso de personalización de urnas carente de un adecuado control de integridad de la información (debido a un defecto del software), es la causa raíz del primer incidente, que desencadenó en una sucesión de acciones e imprecisiones que derivaron finalmente en la suspensión de las elecciones. El defecto no se detectó durante la fase de prueba, debido a que no se realizó un adecuado testing del software. Ya durante la personalización de las urnas, se materializó la falla, puesto que al no contar con el control de integridad, dicho proceso permitió personalizar urnas con la oferta electoral incompleta (no incluía a todos los candidatos). Es por esta razón que el día de las elecciones muchos equipos no contaban con todos los candidatos en el sistema. Cabe señalar que no se hizo un control de calidad antes del despliegue, lo que hubiese permitido detectar la falla oportunamente (antes que se enviasen los equipos a los recintos).

2. La no estandarización de las imágenes coadyuvó a la falla y representa una mala práctica en la gestión de la oferta electoral de procesos con voto electrónico (denominado voto automatizado por la JCE). La oferta electoral a descargar desde los servidores a las urnas durante la personalización era en algunos casos de gran tamaño en bytes.

3. No haber analizado la capacidad de las redes e infraestructura para personalizar el número de urnas previsto (en pocas horas), y el recurrir posteriormente a modalidades no contempladas ni probadas para esta tarea, como el uso de conexiones inalámbricas mediante módems USB, precipitó la falla. La inclusión inicialmente de seis módems 3g afectó a un número menor de urnas y, pese a que no se pudo reproducir la falla durante la auditoría, hay evidencias de que la falta de control de la integridad impidió detectar fallas en la personalización con esta tecnología.

4. Permitir posteriormente el uso de una tecnología inalámbrica como módems 4g sin controles previos ni solicitud de soporte al proveedor, existiendo un antecedente de falla en la personalización de las elecciones primarias (que, según la JCE, fue resuelto en dicha oportunidad como se expresa en el hallazgo 6), resultó determinante para la materialización de la falla. Durante la auditoría, se comprobó un elevado número de personalizaciones incorrectas, fruto del empleo de dicha tecnología; así como también se pudo comprobar la persistencia de la falla reproduciéndola en múltiples ocasiones. Se

reitera, no obstante, que si el procedimiento hubiese contado con el control de integridad, el empleo de esta tecnología no hubiese impactado en el resultado de la personalización.

5. Una vez detectada la falla en la oferta electoral se buscó remediar. Esta actividad fue interrumpida a solicitud de los partidos políticos. Fue un error estratégico estimar que de 5:00 a.m. a 7:00 a.m. del domingo se podía revisar la oferta electoral del voto automatizado en todo el país y remediar las que estuviesen incorrectas.

6. El inicio de la votación con la oferta electoral incorrecta en un grupo importante de colegios electorales demostró una falencia en la comunicación, falta de coordinación del personal a cargo del operativo y una deficiente estrategia de mitigación. Esto configuró una situación insalvable para este grupo importante de mesas que inevitablemente debían anularse posteriormente.

7. La falla en la mitigación, que ocasionó la incorrecta re-personalización al descargar datos de otro colegio electoral en lugar del esperado, terminó por configurar un escenario de desconcierto en el personal técnico; esto, sumado a lo señalado en párrafos precedentes, culminó en la suspensión de las elecciones. Esta falla en la mitigación no fue expuesta a la sociedad, tampoco a los observadores internacionales, ni se incluyó en la relatoría por parte de los técnicos de la JCE. Fue reconocida por el personal técnico de la JCE, luego de que el equipo auditor le comunicase el hallazgo.

8. El limitado porcentaje de colegios electorales que logró iniciar la votación correctamente (sin fallas), sumado a los pocos que pudieron remediar la oferta electoral e iniciar posteriormente, dejó expuesta la incapacidad técnica de mitigar la falla en la totalidad de las urnas ante las situaciones planteadas.

9. Pese a frustrarse el consenso con delegados de los partidos políticos, no existe justificación alguna para no haber implementado un protocolo de control de calidad que contemplase el clonado y la personalización de las urnas. Tampoco hay explicación para la inexistencia de un plan de pruebas (testing) adecuado, que pudo haber detectado la falla a tiempo y, así, evitar esta situación inédita para el país.

10. Los cambios en las candidaturas y la participación activa de las agrupaciones políticas en la definición de los protocolos (no exenta de largas discusiones que en ocasiones

abortaron reuniones importantes), limitó indudablemente las facultades de la Dirección de Informática para la creación unilateral de procedimientos.

11. Fueron analizados los antecedentes, logs, registros de auditoría especiales, configuraciones, control perimetral e informes de seguridad. No se hallaron evidencias de ataques externos.

12. Una vez concluidas las tareas de auditoría en campo y las entrevistas, se analizaron los resultados obtenidos junto a los indicios y evidencias que surgen de la investigación, pudiendo concluir que no se hallaron indicios de sabotaje.

13. El tenor de las fallas y el estado en que se presentaba la oferta electoral (incompleta), no es compatible con un intento de fraude, por lo que se descarta tal intencionalidad.

14. El diseño, desarrollo, prueba y liberación del sistema de voto automatizado, es facultad del área informática de la Junta Central Electoral, así como la ejecución del proceso de personalización de las urnas (incluyendo los recursos humanos y redes involucradas en el mismo). Tanto la materialización de la falla (producto de un defecto de software), que afectó la integridad y la disponibilidad de la información, como el despliegue de equipos en esas condiciones, es por lo tanto responsabilidad de la Dirección de Informática.

15. Existieron otros inconvenientes tecnológicos durante las elecciones municipales. Estos fueron derivados, en su mayoría de los motivos expresados en los hallazgos, como por ejemplo, la falta de procedimientos de control. Entre estos problemas, mencionados anteriormente, se destaca el reporte de que una impresora emitió un voto sin datos impresos (en blanco) y bloqueos de pantalla táctil.

VII. Recomendaciones

Tomando en consideración los hallazgos de esta auditoría, el equipo auditor considera acertada la decisión de no utilizar el sistema de voto automatizado para las elecciones municipales extraordinarias celebradas el 15 de marzo de 2020. Bajo ese mismo criterio, se recomienda no utilizarlo en las próximas elecciones presidenciales programadas para este año.

Con el objetivo de mejorar los procedimientos de diseño, desarrollo e implementación de software, así como la gestión de procesos informáticos de la Junta Central Electoral, el equipo de auditoría brinda las siguientes recomendaciones, cuyo cumplimiento será esencial para evitar la ocurrencia de hechos como los acaecidos en el proceso electoral municipal.

1. Crear un proceso formal para el desarrollo y liberación del software;

2. Elegir un estándar que permita documentar el ciclo de vida del software;

3. Seleccionar un estándar o desarrollar un proceso que facilite la identificación de defectos de software y documente su ciclo de vida;

4. Fortalecer la calidad del software, dado que los principales determinantes de la calidad del software se logran principalmente antes de que comience el testeo.

5. Establecer un procedimiento de testing de software acorde a las aplicaciones críticas que se desarrollan y emplean en la JCE. Se debe capacitar al personal y dotar al área de los recursos necesarios.

6. Determinar los mecanismos de seguridad, niveles de servicio, y requisitos de gestión de todos los servicios de red, generando un adecuado acuerdo de nivel servicios con las empresas proveedoras.

7. Los sistemas a emplear en la JCE deben poseer controles que aseguren tanto la disponibilidad como la integridad de la información en forma continua. En el mediano plazo se deberá establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de continuidad de las operaciones. Esto permitirá a la JCE protegerse, reducir la probabilidad de ocurrencia, prepararse, responder, y recuperarse de incidentes disruptivos cuando acontezcan.

8. Establecer un procedimiento de preservación de todos los artefactos de software a emplear en la elección y sus ítems de configuración. Se debe designar un agente de custodia para guardar los artefactos del sistema de votación (que cuente con el acuerdo de las agrupaciones políticas) y que permita una custodia confiable e independiente.

9. La implementación paulatina de innovaciones tecnológicas, basada en un desarrollo formal del software, acompañada por un riguroso proceso de testing y liberación del sistema, permitiendo que tanto la autoridad electoral como los partidos y la sociedad (con la debida divulgación y capacitación) estén preparados para cambios de tal envergadura.

10. Desarrollar auditorías y evaluaciones independientes como parte de un proceso formal, conocido y debidamente programado, y no como un recurso al que se apela solo ante aquellos eventos que cuestionan la transparencia o efectividad de un sistema informático. Estos ejercicios se deben realizar con suficiente antelación para que puedan realizarse todas las pruebas necesarias para garantizar la robustez y fiabilidad de los sistemas a implementar.

Siglas y Acrónimos

APN: Access Point Name
BCP: Bulk Copy Program
DECO: Departamento para la Cooperación y Observación Electoral
IFES: Fundación Internacional para Sistemas Electorales
JCE: Junta Central Electoral
LAN: Local Area Network (Red de área local)
MOE: Misión de Observación Electoral
OEA: Organización de los Estados Americanos
SFD: Secretaría para el Fortalecimiento de la Democracia
SLA: Service Level Agreement (Acuerdo de nivel de servicio)
SQL: Structured Query Language (Lenguaje de consulta estructurada)
TDS: Tabular Data Stream
TSE: Tribunal Superior Electoral
USB: Universal Serial Bus

Glosario de Términos

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Artefacto de software: Cualquier elemento que resulte del proceso de desarrollo de software, por ejemplo documentos de requisitos, especificaciones, diseños, modelos, descripciones, software, etc.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

Error: Acción huma que produce un resultado incorrecto.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Falla de software: Manifestación física o funcional de un defecto de software.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Impacto: El costo para la organización de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros. Puede reflejarse en pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta.

Log o registro: Es un archivo de texto en el que constan cronológicamente los acontecimientos o eventos que han ido sucediendo en un sistema informático, programa, aplicación, artefacto, servicio o servidor, así como el conjunto de cambios que estos han generado.

Mitigación: Acción de identificar, seleccionar el filtrado y el aislamiento adecuados y neutralizar los efectos de un incidente de seguridad de la información.

Observación: Omisiones, incumplimientos normativos o deficiencias de control interno detectados en la auditoría practicada.

Papeles de Trabajo: Conjunto de documentos que contienen la información obtenida por el equipo auditor en su auditoría, así como los resultados de los procedimientos y pruebas de auditoría aplicadas. Con ellos se sustentan las observaciones, recomendaciones y conclusiones contenidas en los informes correspondientes.

Protocolos de red: Conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red de datos. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas respecto al formato determinan si los datos son recibidos correctamente, si ha ocurrido algún tipo de problema en la transferencia de la información o son rechazados por el destinatario.

Recomendación: Propuesta hecha al auditado con la finalidad de prevenir o corregir la reincidencia de las observaciones determinadas, que elimine las causas que las originaron o que promuevan una mejora.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Seguimiento: Es la acción de constatar que las recomendaciones planteadas se hayan cumplido en tiempo y forma, verificando el avance en la atención o solución definitiva a la problemática detectada.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Testing o prueba de software: Es el proceso de estudio de un programa o artefacto con la intención de encontrar errores.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.