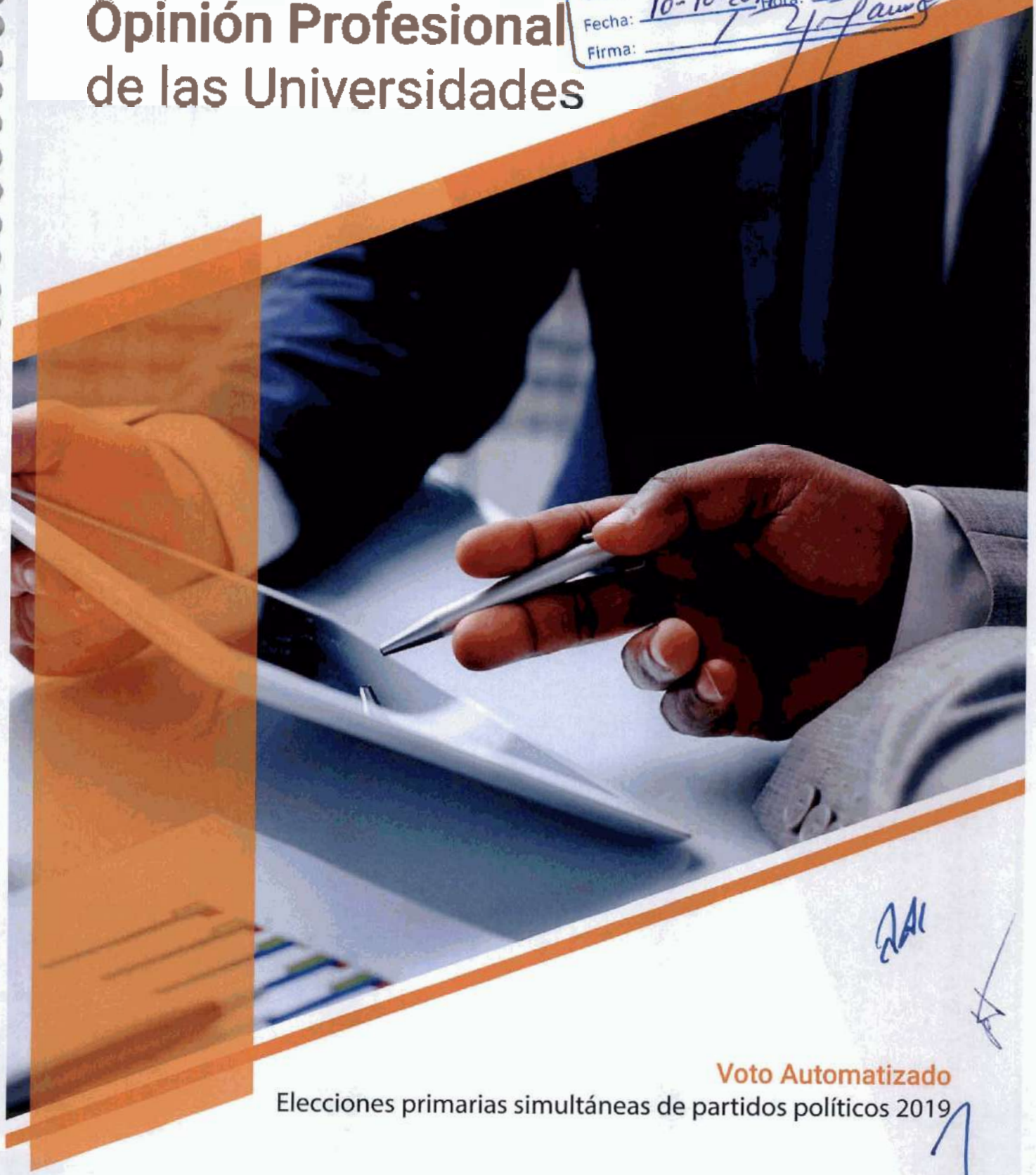
Opinión Profesional de las Universidades



Voto Automatizado

Elecciones primarias simultáneas de partidos políticos 2019

UNIBE ITLA intec PUCMM

Índice

Voto Automatizado

Elecciones Primarias Simultáneas de Partidos Políticos 2019.

Opinión Profesional

Universidades:

ITLA - Instituto Tecnológico de Las Américas.

INTEC - Instituto Tecnológico de Santo Domingo.

UNIBE - Universidad Iberoamericana.

PUCMM - Pontificia Universidad Católica Madre y Maestra.

27-09-2019

Santo Domingo, D.N.

República Dominicana.

ANTECEDENTES

La Junta Central Electoral, con la intención de garantizar la integridad y la transparencia de las primarias simultáneas de los partidos políticos a celebrarse el próximo 6 de octubre del 2019, a través de su presidente, el Dr. Julio César Castaños Guzmán, solicita a los rectores del: Instituto Tecnológico de Las Américas - ITLA, Instituto Tecnológico de Santo Domingo - INTEC, Universidad Iberoamericana - UNIBE y la Pontificia Universidad Católica Madre y Maestra – PUCMM, su colaboración para generar un informe de observaciones por parte de sus respectivos equipos técnicos, enfocado en garantizar el cumplimiento de 3 grandes pilares:

1. ***Que el Sistema de Voto Automatizado garantiza el Voto Secreto de los electores.***

2. ***Comprender que dicho sistema funciona operativamente sin conexión a internet y que puede ser conectado a una red privada de prestadoras de servicios telefónicos al momento de dar el Boletín Cero y, una vez se proceda a la impresión y transmisión de los Resultados.***

3. ***Verificar que es auditable y comprobable que la sumatoria de los votos físicos depositados en las urnas de las mesas de votación, coinciden con lo expresado en el Acta Final de los resultados de la mesa.***

Para lograr el objetivo, los equipos técnicos de las Instituciones de Educación Superior - IES, iniciaron jornadas de trabajo en compañía de sus homólogos en la Junta Central Electoral, por espacio de 4 días, dado al corto tiempo con el que dispone la entidad electoral, para la configuración de las 7,372 estaciones de trabajo que participarán del proceso.

CRONOLOGÍA DE EVENTOS

Para dar inicio a los trabajos, fueron creadas 3 comisiones con especial interés en garantizar el cumplimiento de los objetivos primarios, antes expuestos, dando como resultados tres (3) equipos de trabajo. A continuación, detalles cronológicos de las actividades:

Miércoles 18-9-2019:

Presentación inductora por parte del Dr. Castaños a los técnicos y rectores de las diferentes Instituciones de Educación Superior – IES, e inicio de mesas generales de trabajo para conocer el proceso, desde la óptica del usuario final.

Jueves 19-9-2019:

Continuidad de los trabajos por presentación del producto, en esta ocasión con un enfoque técnico, y creación de los equipos de especialistas y plan de trabajo a seguir por disciplina de dominio.

- **Seguridad en términos de Infraestructura.**
- **Seguridad en términos de transmisión de data.**
- **Trazabilidad de la Plataforma (Encriptación y Manejo de la Data).**

Viernes 20-9-2019:

Continuidad a las sesiones de trabajo, con demostraciones, paneles de preguntas y respuestas y solicitud de entregables e insumos requeridos.

Sábado 21-9-2019:

Sesión de trabajo para recepción de documentación solicitada y validación de reportes finales en servidor central.

2. Operatividad fuera de línea:

Objetivo

Comprender que dicho sistema funciona operativamente sin conexión a internet y que puede ser conectado a una red privada de prestadoras de servicios telefónicos al momento de dar el Boletín Cero y, una vez se proceda a la impresión y transmisión de los Resultados.

Verificación

Se realizaron verificaciones de operatividad desde 2 perspectivas diferentes: Hardware, Seguridad de Transmisión e Integridad de la Data.

Resultado

Satisfactorios con recomendaciones que no afectan el proceso. A continuación, detalles por tópicos:

- **Computador de escritorio:** este equipo será empleado para realizar el voto para parte de los electores. Es de tecnología táctil y su teclado físico fue inactivado. El mismo cuenta con la instalación del O.S. Microsoft Windows 10 Pro.
- **Laptop Ultrabook:** este equipo será utilizado por los presidentes de las mesas para el escaneo de las cédulas. El mismo cuenta con la instalación del O.S. Microsoft Windows 10 Pro.
- **Impresora Térmica:** utilizada para imprimir el sufragio de los electores. Presenta los controles de lugar para asegurar la impresión de los mismos. Responde de forma adecuada a la falta de insumos o fallas de energía.
- **Inversor:** unidad con autonomía de 12 horas, suficientes para asegurar el proceso.
- **Lector de barra:** Empleado para la lectura de los códigos de barra en los documentos de identidad.
- **Memoria USB:** empleada para mantener copia local de la base de datos manejada en el centro electoral.

LEVANTAMIENTOS POR OBJETIVOS

En este apartado, desarrollamos los tres pilares requeridos de forma detallada:

1. No trazabilidad en captura de votos:

Objetivo

Asegurar que la aplicación no registra datos de los votantes en cumplimiento con la ley sobre el secreto del voto.

Verificación

Se realizaron verificaciones conectados en la base de datos central y la base de datos local.

Resultados

Satisfactorio. En ambos caso, local y servidor central, se pierde la posibilidad de saber el voto realizado por el elector. Esto es logrado por dos estrategias:

- Existen dos esquemas de datos diferentes (que contienen los electores y votos respectivamente), ambos esquemas NO guardan relación entre sí, y sus datos son re-sorteados cada vez que se genera un nuevo voto. Evitando a su vez, se detectado el votante y su preferencia por la hora de llegada al centro.
- Cada voto es identificado por un "NewID", función provista por el gestor de bases de datos de Microsoft SQL SERVER, que le otorga un identificador único global, garantizado por la regulación RFC 4122.
- De igual forma, se realizaron pruebas en el código QR y en el hash generado en las boletas impresas, para garantizar que no haya rastreo del elector, pudiendo comprobar que sólo son transmitidos datos generales de la mesa de votación.

- **Celular:** empleado para la comunicación técnica y como medida de contingencia para la transmisión de los datos.
- **Servidores de Base de datos:** Fueron verificados los servidores físicos y mostrados los niveles de contingencia, redundancia y alta disponibilidad con que cuenta la Junta Central Electoral - JCE para garantizar el proceso de votación. De igual forma, fueron solicitadas las informaciones siguientes:
  - Protocolos y mecanismos de accesos y seguridad a las DB.
  - Cantidades de sesiones concurrentes que pueden manejar.
  - Mecanismos para evitar DDoS.
    Arquitectura para el balanceo de carga y Alta disponibilidad.
  - Arquitectura en la nube para accesos a los datos para los partidos.
  - Control de accesos y bitácora de accesos a la base de datos.

- **Seguridad de Transmisión e Integridad de la Data:** Se observó la demo del equipo técnico sobre la simulación de una votación y el cierre al final del proceso de votación; enviando los resultados del proceso por el mecanismo normal de la línea de comunicación APN mediante el dispositivo de activación USB 3G/4G en una mesa ficticia, y por la vía alterna haciendo uso la app instalada en el Smartphone que lee el código QR generado por el sistema (como mecanismo alterno ante fallas del mecanismo principal).

  Para ambos casos, el sistema permite realizar la trasmisión en momentos diferentes, realizando inserción del resultado de la votación en la base datos del Servidor central.

  Se pudo observar que no se duplica la data, pues siempre que se transmitan prevalecerá la transmisión desde el computador y no desde la contingencia, pero si se registran las transmisiones.

  La transmisión primaria la realiza vía línea adscrita al APN y la del aplicativo móvil la realiza a una carpeta offline de la data que se envía por la app del celular autorizado.

3. Garantizar que los resultados sean auditables

Objetivo

Verificar que es auditable y comprobable que la sumatoria de los votos físicos depositados en las urnas de las mesas de votación coinciden con lo expresado en el Acta Final de los Resultados de la mesa.

Verificación

Se realizaron verificaciones en plataforma demostrativa comparando base de datos local y base de datos en servidor central contra los votos impresos.

Resultados

Satisfactorio. En ambos caso local y servidor central, los datos reflejados en la base de datos local y en los dashboards del servidor central, comprobaron obtener la cantidad de votos realizados en las pruebas demostrativas.

RECOMENDACIONES A LOS PROCESOS

Luego de los trabajos y observaciones realizadas a los procesos, el equipo de trabajo realiza las recomendaciones siguientes:

1. Equipamiento en la Terminal

Equipo Desktop Mini PC:

a) Deben poseer un sistema de manejo de end-point de seguridad y manejo de riesgo ante robo. ***Respuesta satisfactoria según requerimiento 16 del Anexo: Reparos y Comentarios a las Sugerencias.***

b) Deben implementar un procedimiento de manejo de credenciales de accesos al equipo, para evitar un único usuario y contraseña para los 7,273 pc.

c) Bloquear los puertos y servicios del pc que no estén en uso. Puede ser por cinta adhesiva o software, como el ya empleado en la plataforma de móviles como lo es Manage Engine. Ver (https://www.manageengine.com/es/it-compliance-suite.html?me-homesoln). *Recuperado: 26-09-2019.* ***Respuesta satisfactoria según requerimiento 18 del Anexo: Reparos y Comentarios a las Sugerencias.***

d) Se solicita nos provean el criterio de generación de estaciones a ser auditadas en el proceso. Se sugiere la construcción de este procedimiento para el criterio de generación de las estaciones que serán auditadas. ***Respuesta satisfactoria según Requerimiento 8, del Anexo de Reparos y Comentarios a las Sugerencias.***

e) Realizar pruebas aleatorias de seguridad en los equipos clonados, tomando como base, el checklist de políticas aplicadas. ***Respuesta satisfactoria según requerimiento 19 del Anexo: Reparos y Comentarios a las Sugerencias.***

f) Se sugiere que los equipos que vayan a ser utilizados como sustitución, estén registrados en la base de datos, para que cualquier equipo (CPU) que se integre debido a fallo, asegure que el dispositivo a conectar este validado (al margen de que pudimos apreciar los niveles de validación con la integración de los nuevos equipos en el

escenario en el cual se hace necesario sustituir). Entendemos que este punto añade mayor seguridad al proceso. ***Respuesta satisfactoria según requerimiento 20 del Anexo: Reparos y Comentarios a las Sugerencias.***

Laptop Ultrabook:

a) Deben poseer políticas locales y centralizadas para la gestión de puertos de accesos. ***Respuesta satisfactoria según requerimiento 22 del Anexo: Reparos y Comentarios a las Sugerencias.***
b) Deben poseer un sistema de manejo de end-point de seguridad y manejo de riesgo ante robo.
c) Deben implementar un procedimiento de manejo de credenciales de accesos al equipo, para evitar un único usuario y contraseña para los 7,273 pc.
d) Bloquear los puertos y servicios del pc que no estén en uso. Puede ser por cinta adhesiva o software, como el ya empleado en la plataforma de móviles como lo es Manage Engine. Ver (https://www.manageengine.com/es/it-compliance-suite.html?me-homesoln). Recuperado: 26-09-2019.

Inversor:

a) Considerar el bloqueo de las tomas disponibles para evitar la conexión de equipos que son partes del proceso que puedan hacerle fallar por el sobre-consumo. ***Respuesta satisfactoria según requerimiento 9 del Anexo: Reparos y Comentarios a las Sugerencias.***

Memoria USB:

a) Recomendamos tener un modelo de encriptación que impida su reproducción en otros escenarios. ***Respuesta satisfactoria según Requerimiento 23, del Anexo de Reparos y Comentarios a las Sugerencias.***

b) Se recomienda estampar las memorias porque son genéricas para una mejor identificación. ***Respuesta satisfactoria según Requerimiento 24, del Anexo de Reparos y Comentarios a las Sugerencias.***

c) Se recomienda incluir un proceso de notificación en caso de posible desconexión. ***Respuesta satisfactoria según Requerimiento 10, del Anexo de Reparos y Comentarios a las Sugerencias.***

d) Recomendamos un procedimiento para enrolamiento de las memorias con las terminales. ***Respuesta satisfactoria según requerimiento 25 del Anexo: Reparos y Comentarios a las Sugerencias.***

Celulares:

a) Se recomienda la creación de un procedimiento donde muestre la relación de Celular serial, IMEI y APN con la plataforma del ISP y software de gestión de los equipos. ***Respuesta satisfactoria según requerimiento 15 del Anexo: Reparos y Comentarios a las Sugerencias.***

2. Seguridad de Transmisión e Integridad de la Data:

a) Se recomienda un mecanismo de control de software que evite la doble transmisión, es decir, una vez se envíe por APN, no permita enviar por la app del Smartphone y viceversa. Aun cuando se validó que la data NO SE DUPLICA, permite retransmitir (y esto puede generar duda razonable en uno de las partes interesadas que no conozcan los controles que están implementados). ***Respuesta satisfactoria según requerimiento 11 del Anexo: Reparos y Comentarios a las Sugerencias.***

b) Se recomienda que los equipos de respaldo también estén inscritos de forma controlada al igual que los equipos en operación, para que el protocolo de sustitución asegure que sea dispositivo controlado. ***Respuesta satisfactoria según requerimiento 21 del Anexo: Reparos y Comentarios a las Sugerencias.***

c) Se recomienda emitir anexos de erratas cuando sea modificado alguno de los pasos en el instructivo, para asegurar el cumplimiento de las responsabilidades de los miembros

de la mesa de votación. ***Respuesta satisfactoria según requerimiento 26 del Anexo: Reparos y Comentarios a las Sugerencias.***

d) Realizar pruebas aleatorias de seguridad en los equipos clonados, tomando como base, el checklist de políticas aplicadas.

e) Se recomienda solicitar garantías firmadas de seguridad y monitoreo de los servicios entregados por los proveedores CLARO y ALTICE, previo-durante-posterior a la jornada. ***Respuesta satisfactoria según requerimientos 28 y 29 del Anexo: Reparos y Comentarios a las Sugerencias.***

3. Resultados sean auditables:

a) Se recomienda poner los reportes pre-hechos como disponibles en el espacio de repositorio en la nube (AZURE) para que los usuarios autorizados a este espacio puedan ver los dashboards. ***Respuesta satisfactoria según requerimiento 12 del Anexo: Reparos y Comentarios a las Sugerencias.***

4. Software Voto Automatizado:

a) Se sugiere construir un procedimiento documentado de sustitución de equipos en caso de fallo, en las estaciones de votación (considerar cualquiera de los equipos). ***Respuesta satisfactoria según requerimiento 13 del Anexo: Reparos y Comentarios a las Sugerencias.***

b) Se recomienda trabajar en un procedimiento para el control de cambio de las versiones del aplicativo vitales en el proceso. ***Respuesta satisfactoria según requerimiento 27 del Anexo: Reparos y Comentarios a las Sugerencias.***

c) Se recomienda tener un procedimiento para auditar a las telefónicas en materia de seguridad de la información que se estará transmitiendo por dichas plataformas. ***Respuesta satisfactoria según requerimientos 28 y29 del Anexo: Reparos y Comentarios a las Sugerencias.***

d) Se sugiere que los dashboards con data resumida, sean puesto a la disposición de los stakeholders externos que tendrán acceso a la data cruda, para que todos tengan la capacidad de mirar la información al mismo tiempo en las formas y formatos que utiliza la JCE en sus dashboards. ***Respuesta satisfactoria según requerimiento 13 del Anexo: Reparos y Comentarios a las Sugerencias.***

5. Servidor y gestor de base de datos: fueron requeridas las documentaciones que garanticen el cumplimiento de los puntos siguientes:

a) Protocolos y mecanismos de accesos y seguridad a las DB. ***Respuesta satisfactoria según requerimiento del Anexo: Reparos y Comentarios a las Sugerencias.***

b) Cantidades de sesiones concurrentes que pueden manejar. ***Respuesta satisfactoria según requerimiento del Anexo: Reparos y Comentarios a las Sugerencias.***

c) Mecanismos para evitar DDoS. ***Respuesta satisfactoria según requerimiento del Anexo: Reparos y Comentarios a las Sugerencias.***

d) Arquitectura para el balanceo de carga y Alta disponibilidad. ***Respuesta satisfactoria según requerimiento del Anexo: Reparos y Comentarios a las Sugerencias.***

e) Arquitectura en la nube para accesos a los datos para los partidos. ***Respuesta satisfactoria con las observaciones siguientes: recomendamos implementar los mismos controles que se implementaron para la infraestructura interna para la denegación de servicio, ya que un posible ataque al espacio compartido en la nube de la generación de datos en línea, si bien no afecta el proceso electoral, puede afectar la credibilidad del proceso.***

f) Control de accesos y bitácora de accesos a la base de datos. ***Respuesta satisfactoria según requerimiento del Anexo: Reparos y Comentarios a las Sugerencias.***

6. Normativas:

a) Se recomienda que la Junta Central Electoral – JCE, se aboque a la adopción de normativas que permitan trabajar con aspectos de gestión de calidad / documentación / gobernanza de TI. Esto, envolviendo a los jugadores que al momento de originar el proceso entiendan pertinentes. ***Según requerimiento 14, La JCE estará acogiendo el sistema de gestión de calidad ISO 9001:2015 y la normativa de procesos electorales ISO 17582:2014***

CONCLUSIÓN

Los 3 focos primordiales que fueron objetos de esta revisión profesional a los fines de garantizar la No trazabilidad de votos, conectividad fuera de línea y auditoria del conteo de votos, por parte de los representantes de las Instituciones de Educación Superior – IES, arrojaron resultados **SATISFACTORIOS** al momento del cierre de los procesos de evaluación en fecha 21 de septiembre del 2019. Presentando en adición, observaciones y oportunidades de mejora en la documentación de los procesos y las operaciones en campo.

Los pilares observados (Hardware, Aplicativo, y Transmisión de datos) **FUNCIONAN CORRECTAMENTE** y como técnicos recomendamos validar las observaciones puntuales emitidas en el detalle de este documento, a los fines de garantizar la efectividad del proceso.

FIRMA DE PARTICIPANTES

Ing. José Armando Tavarez

ITLA - Instituto Tecnológico de Las Américas

Dr. Rolando Guzmán

INTEC - Instituto Tecnológico de Santo Domingo

Dr. Julio Amado Castaños Guzmán

UNIBE - Universidad Iberoamericana

Dr. Alfredo de la Cruz Baldera

PUCMM - Pontificia Universidad Católica Madre y Maestra

****** Fin del documento de las recomendaciones*****

Anexos

Reparos y Comentarios a las Sugerencias Contenidas en el Documento de la Opinión Profesional Emitida por las Universidades Sobre el Módulo de Votación Automatizada Elecciones Primarias 2019

Reparos y Comentarios a las Sugerencias Contenidas en el Documento de la Opinión Profesional Emitida por las Universidades Sobre el Módulo de Votación Automatizada Elecciones Primarias 2019

30 de septiembre de 2019

Recomendaciones y Sus Repuestas

1. **Requerimiento: Mecanismos para evitar DDoS.**

   Respuesta: El factor de riesgo para un ataque de este tipo es mínimo en la red del Voto Automatizado, dado que la misma no está expuesta al internet y las comunicaciones se realizan mediante un APN privado con diferentes proveedores de servicios. Solamente está permitido el tráfico de SIM Cards registradas y las conexiones son recibidas en equipos de filtrado de contenido y control de tráfico, como son: Firewalls, Sistemas de detección y prevención de Instrucción (IDS e IPS) para la protección de las capas de 1-4 del modelo OSI.

   Para las capas de bajo nivel (5-7) se dispone de equipos de control de entrega de aplicaciones (ADC), previniendo los ataques de desborde de conexiones y sesiones, así como las solicitudes maliciosas.

   Las políticas implementadas incluidas son las siguientes:

   a) Denegación por defecto de paquetes no definidos por reglas de acceso.
   b) Validación de protocolo de comunicación
   c) Límite de frecuencia de conexiones

2. **Requerimiento: Balanceo de Carga y Alta Disponibilidad.**

   Respuesta:

   Se disponen de dos balanceadores físicos de carga en modo proxy, los cuales reciben y distribuyen el tráfico a los servidores de base de datos. El clúster de equipos dispone de una capacidad de respuesta (total) de 10Gbps de throughput (L7) y 750,00 req/seg (L7).

   Se disponen de replicaciones activas y pasivas de los servidores de base de datos, los cuales están alojados en una nube privada (multi-site) con hypervisores redundantes. Habrá tres réplicas de la base de datos: Una local, una en un sitio remoto y una parcial en Azure

3. **Requerimiento: Arquitectura en la Nube para accesos a los datos para los partidos.**

   Respuesta:

   Para las conexiones en la nube se dispone de lo siguiente:

   a) Conexión multipunto a servidor de base de datos en la nube para la sincronización de los datos recibidos.
   b) Conexiones privadas para cada partido a instancias específicas de base de datos y portales de resultados (Dashboards)
   c) Data Warehouse en nube para la generación de reportes y despliegue de resultados individuales de manera inmediata.
   d) Utilización de Data Factory para la individualización y perfilamiento de los datos almacenados.

4. **Requerimiento: Mecanismos de accesos y Seguridad a las DB**

Respuesta:

a) El acceso a la base de datos se realiza mediante un único usuario, a través de la aplicación. Este usuario solo posee permisos para ejecutar procedimientos y realizar lecturas.

b) El día de las elecciones se define un usuario para realizar las tareas administrativas de la base de datos (respaldo, replicación, monitoreo de la base de datos, etc.)

c) Los usuarios administrativos de la base de datos (sa, administrador) se deshabilitan y se crea un usuario con los mismos privilegios, pero con una clave compuesta de dos partes custodiadas por separados. Los custodios son personas designadas por la Dirección de Informática.

5. **Requerimiento: Cantidad de sesiones concurrentes que pueden manejar**

Respuesta:

a) La versión de SQL Server utilizada es la versión Enterprise 2017 licenciada por Core, en esta versión el número de conexiones simultaneas permitidas depende de la configuración del server (memoria y números de Core) y la aplicación que se esté utilizando.

b) El servidor que se está utilizando es un servidor virtual que nos permite aumentar sus capacidades en línea (memoria y Core), lo que nos permitiría aumentar el número de secciones concurrentes máximas permitidas.

c) Basada en la estimación de conexiones simultaneas esperadas y las capacidades iniciales de la máquina virtual, se mantuvo la configuración sugerida de SQL Server de 32,767 conexiones como máximo, lo cual supera en más de un 100% las conexiones concurrentes esperadas.

6. **Requerimiento: Control de accesos y bitácora de accesos a la base de Datos**

Respuesta:

(A) El acceso a la base de datos contempla tres niveles de seguridad:

1. Las mesas se estarán conectando al servidor utilizando un usuario que solo puede ejecutar procedimientos almacenados, sin ningún otro privilegio.
2. Se habilita un trigger logon que solo permite que usuarios autorizados y aplicaciones autorizadas puedan conectarse a la base de datos. Esto evita que un usuario intente correr una aplicación no autorizada o utilizar el SQL Management, u otra aplicación de terceros similar, para acceder a la base de datos

d) Los usuarios tradicionales de administración de SQL son deshabilitados y se crea un nuevo usuario con los privilegios de SA, pero con una clave compuesta de dos partes custodiadas por separados. Dichos custodios son personas designadas por la Dirección de Informática.

(B) En cuanto a la bitácora de accesos se habilitan dos categorías de auditoria:

- Nivel de servidor. Se registran todos los cambios de administración y los inicios y cierres de sesión, además de los intentos de inicio fallidos.
- Nivel de base de datos. Se registran todos los cambios a nivel de manipulación de datos (DML) y de definición de datos (DDL).

7. **Requerimiento: Equipos de la Terminal, Equipo Thin Client.**

   Respuesta: La JCE hace la observación con relación al equipo catalogado como Thin Client, el cual en realidad es una **Desktop Mini PC,** que funciona de manera standalone.

8. **Requerimiento: Acápite D.** Criterio de Generación de estaciones a ser auditadas en el proceso.

   Respuesta:

   El método incluyó cuatro pasos desagregados que permitieron una distribución proporcional del 20% a nivel nacional en sobres no identificados que fueron introducidos de forma aleatoria en las valijas correspondientes a cada mesa electoral.

   Procedimiento:

   a. Con el uso de una herramienta informática, se determinó la cantidad de mesas a auditar en cada uno de los municipios, para asegurar la distribución equitativa y proporcional de la muestra a nivel nacional, consistente en el 20% de las mesas de cada municipio y el Distrito Nacional.

   b. Se imprimieron 7,372 volantes, equivalentes al número total de mesas, con la aplicación de un método de impresión aleatoria con los enunciados de si en esa mesa corresponde auditoría o no.

   c. Dichos volantes fueron introducidos en sobres no identificados. En el proceso de etiquetado para fines de línea de producción, se tuvo la previsión, conforme sugerencia de los partidos políticos, que no fuera posible establecer ninguna secuencia.

   d. Los 7,372 sobres fueron insaculados según la distribución determinada por municipio. Posteriormente, cada sobre fue seleccionado mediante sorteo manual simple, realizado al azar, de entre la totalidad de sobres correspondientes al municipio, y fue introducido en cada valija en la línea de producción y en presencia de delegados de los partidos políticos.

   Con la implementación de dicho método de aleatoriedad, cada sobre fue introducido en la valija sin que se pudiera determinar el contenido del mismo.

9. **Inversor:**

a) **Considerar el bloqueo de las tomas disponibles para evitar la conexión de equipos que son partes del proceso que puedan hacerle fallar por el sobre-consumo.**

Respuesta: El inversor en la actualidad posee cuatro tomas de corriente para alimentación AC, los cuales son ocupados por las cuatro fuentes de los dispositivos que conforman el módulo de votación automatizado, no dejando espacio para conexión de otro dispositivo que pueda generar una sobre carga.

Detalle de Fuentes:

1. Fuente de Laptop HP.

a) Fuente de Mini CPU.

b) Fuente de Monitor Táctil.

c) Fuente Impresora Térmica HP.

10. **Memoria USB:**

c) **Se recomienda incluir un proceso de notificación en caso de posible desconexión.**

Respuesta: La estación de verificación indica cuando el USB de BackUp, tanto de la Urna de Votación como de la propia Estación de Verificación, está desconectado o fallando. Del mismo modo, esta alerta desaparece cuando la memoria USB es conectada nuevamente al equipo.

11. **Seguridad de Transmisión e Integridad de la Data:**

a) **Se recomienda un mecanismo de control de software que evite la doble transmisión, es decir, una vez se envíe por APN no se permita enviar por la app del Smartphone y viceversa. Aun cuando se validó que la data NO SE DUPLICA, permite retransmitir (y esto puede generar duda razonable en uno de las partes interesadas que no conozcan los controles que están implementados).**

Respuesta: Estas recomendaciones se encuentran implementadas en la versión 2.0.0.0 de producción, en la cual se implementó que el sistema no permita la retransmisión vía APN. En caso de intentar retransmitir, el sistema alerta al usuario con el mensaje de que los datos fueron transmitidos y no es necesario volverlo a intentar. En cuanto a la transmisión vía el dispositivo móvil, mediante la captura del código QR, la misma es recibida, pero no realiza ninguna modificación a los datos previamente recibidos, siempre y cuando se hagan referencia a la misma información.

12. **Resultados sean auditables:**

- Se recomienda poner los reportes pre-hechos como disponibles en el espacio de repositorio en la nube (AZURE) para que los usuarios autorizados a este espacio puedan ver los dashboards.

Respuesta: Este proceso se encuentra en fase de implementación, por lo cual, desde hace aproximadamente tres meses, estamos trabajando con los partidos políticos que van a participar en las primarias 2019, sobre el uso de la herramienta PowerBI Embeded, para la publicación de resultados en la página de la JCE, la cual servirá de consulta para los partidos políticos, medios de comunicación y público en general.

13. **Software Vote Automatizado:**

a) **Se sugiere construir un procedimiento documentado de sustitución de equipos en caso de fallo, en las estaciones de votación (considerar cualquiera de los equipos).**

Respuesta: Sugerencia acogida, fue elaborado un procedimiento para la sustitución de equipos del módulo de votación automatizada, donde se especifica la manera de proceder ante la necesidad de sustituir un componente que presente un fallo o daño. En adición se diseñó un check-List para control de los equipos a sustituir. *Ver Anexo*

d) **Se sugiere que los dashboards con data resumida, sean puesto a la disposición de los stakeholders externos que tendrán acceso a la data cruda, para que todos tengan la capacidad de mirar la información al mismo tiempo en las formas y formatos que utiliza la JCE en sus dashboards.**

Respuesta: Esta solución está en proceso de implementación en conjunto con los partidos políticos. Ya se han efectuado varias reuniones con los delegados técnicos y políticos de los partidos, para discutir el proceso de recepción y consulta de la información en Azure, tanto de la data cruda, como los reportes o Dashboards informativos. Se les entregó la arquitectura de comunicación y la estructura de datos donde se estarían recibiendo las informaciones.

14. **Normativas:**

a) **Se recomienda que la JCE se aboque a la adopción de normativas que permitan trabajar con aspectos de gestión de calidad / documentación / gobernanza de TI. Esto, envolviendo a los jugadores que al momento de originar el proceso entiendan pertinentes**

Respuesta: Hemos acogido la norma ISO de calidad 9001:2015 y de gestión de procesos Electorales ISO 17582:2014.

15.. **Celulares:**

a) **Se recomienda la creación de un procedimiento donde muestre la relación de Celular serial, IMEI y APN con la plataforma del ISP y software de gestión de los equipos.**

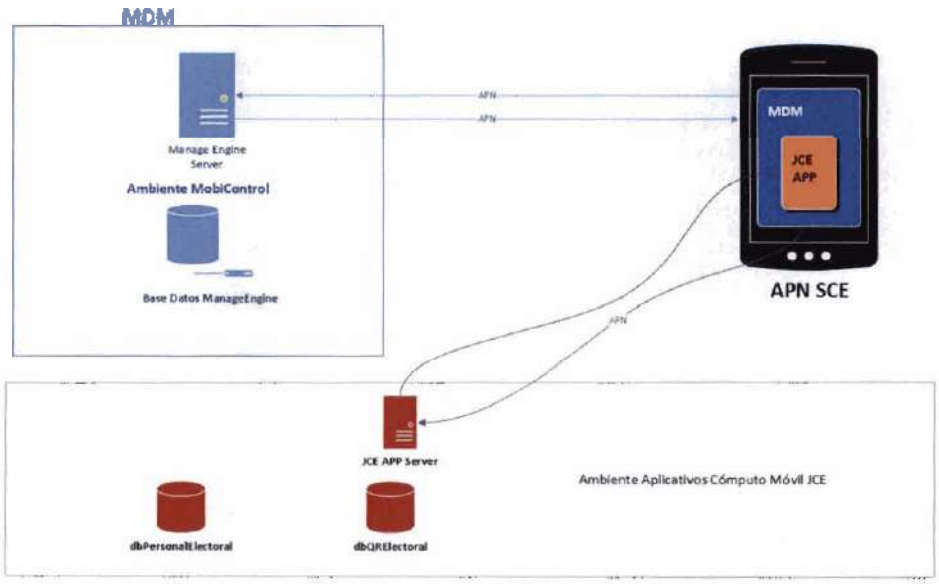
Respuesta: Los dispositivos están conectados a través del APN privado de la JCE para el proceso electoral. Cada uno es aprovisionado con una configuración de seguridad a través de la plataforma Manage Engine (MDM), la cual autoriza el dispositivo a través de su IMEI dentro de la plataforma y luego el dispositivo es colocado en un grupo de trabajo el cual determina los permisos y aplicaciones que tendrá disponible el usuario de este dispositivo.

A través de esta plataforma se puede controlar un dispositivo, enviar actualizaciones y modificar permisos uno a uno o en grupo. Los dispositivos incluyen una SIM CARD provista por el proveedor servicio, en este caso (Claro y Altice). Previa validación, sólo son autorizadas las conexiones a través de los SIM CARD cuyos IMSI (International Mobile Subscriber Identity) están registrados en la lista de acceso tanto de la plataforma del proveedor de servicios como en la plataforma MDM de la JCE.

Mediante procedimientos establecidos, se determina:

1) Si la transmisión fue realizada por un dispositivo autorizado.
2) Si el usuario del dispositivo está previamente autorizado para trabajar en el proceso.
3) Si un QR es válido o no.
4) Si fue recibido previamente y su clasificación.

Ambiente Aplicaciones Móviles JCE



16. Deben poseer un sistema de manejo de end-point de seguridad y manejo de riesgo ante robo.

Respuesta:

La naturaleza de funcionamiento de los equipos es en modo fuera de línea, lo que limita el empleo de este tipo de herramienta, que por lo general son consolas centralizadas para la administración de los equipos conectados a la red. En vista de que los equipos solamente se conectan a la sede central de la JCE, mediante la colocación manual de un modem USB para la transmisión puntual del Test de la Urna, Boletín Cero y Boletín Final. Como sustituto de un aplicativo tipo end-point, se está utilizando Windows Defender, con todas las características de protección habilitadas, más las restricciones aplicadas por políticas de seguridad.

El factor de exposición de estos sistemas se encuentra minimizado en caso de robo o pérdida, en vista de que los equipos tienen seguridad aplicada en el BIOS que limita el acceso a las funciones administrativas y elimina la posibilidad de iniciar el mismo con algún utilitario para poder accesar el disco en un ataque del tipo cold boot y se ha aplicado encriptación al disco duro con un nivel de protección AES 256, en adicción el uso de chip de seguridad TPM 2.0 integrado en la misma.

Para mitigar el riego ante un robo o pérdida del equipo, se han aplicado políticas de seguridad al Sistema Operativo y endurecimiento de la configuración acorde a estándares y mejores prácticas de la industria, las cuales garantizan que el sistema solamente pueda ser utilizado por los usuarios previamente autorizados. De la misma forma si el equipo resultare comprometido, el atacante no podría acceder a la información contenida en el mismo, por la encriptación aplicada.

17. Deben implementar un procedimiento de manejo de credenciales de accesos al equipo, para evitar un único usuario y contraseña para los 7,273 PC.

Respuesta:

Para Acceder al sistema es obligatoria la incorporación de dos passwords (presidente y secretarios de la mesa), que son generados de forma aleatoria y son diferentes para cada mesa de votación.

18. **Bloquear los puertos y servicios del pc que no estén en uso. Puede ser por cinta adhesiva o software, como el ya empleado en la plataforma de móviles como lo es Manage Engine. Ver (https://www.manageengine.com/es/it-complíancesuite.html?me-homesoln). Recuperado: 26-09-2019.**

Respuesta:

El sistema operativo está configurado solamente con los servicios básicos necesarios para el funcionamiento del aplicativo del voto Automatizado y tiene restringido la instalación de cualquier driver o aplicativo fuera de los ya establecidos. Este tiene una función combinada con las políticas del sistema operativo que permite la ejecución solo de los programas preestablecidos.

Con relación a la suite de manageengine recomendada, pudimos verificar que la misma está orientada a equipos conectados a una red o dominio centralizado. El esquema desarrollado por la JCE aplica a un modelo offline stand alone, por lo que un manejo centralizado no aplica para este tipo proyecto y dificultaría su implementación.

Consideramos valida esta recomendación de controlar los puertos y dispositivos, por lo que evaluaremos diferentes opciones del mercado, para futuras versiones, considerando que las mismas funcionan de manera centralizada y el voto automatizado funciona fuera de línea.

19. **Realizar pruebas aleatorias de seguridad en los equipos clonados, tomando como base, el checklist de políticas aplicadas.**

Respuesta:

Parte de los procedimientos establecidos para el desarrollo de software es hacer evaluaciones sobre las políticas de seguridad aplicadas. Para ello de forma aleatoria se prueban muestras en la línea de producción. Se elaboró un formulario de control tipo Check-List para verificar que las políticas de seguridad establecidas fueron aplicadas correctamente al equipo modelo para la clonación y reproducción del mismos. Como es un proceso de clonación, todas las políticas aplicadas al equipo plantilla son replicadas bit por bit a las maquinas destinos.

20. **Se sugiere que los equipos que vayan a ser utilizados como sustitución, estén registrados en la base de datos, para que cualquier equipo (CPU) que se integre debido a fallo, asegure que el dispositivo a conectar este validado (al margen de que pudimos apreciar los niveles de validación con la integración de los nuevos equipos en el escenario en el cual se hace necesario sustituir, este punto del registro entendemos que podría añadir aún más seguridad al proceso).**

Respuesta:

Recomendaciones Acogidas y aplicadas para las primarias del 6 octubre 2019.

21. Se recomienda que los equipos de respaldo también estén inscritos de forma controlada al igual que los equipos en operación, para que el protocolo de sustitución asegure que sea dispositivo controlado.

Respuesta:

Recomendaciones Acogidas y aplicadas para las primarias del 6 octubre 2019.

22. Deben poseer políticas locales y centralizadas para la gestión de puertos de accesos.

Respuesta:

El sistema operativo está configurado solamente con los servicios básicos necesarios para el funcionamiento del aplicativo del voto Automatizado y tiene restringido la funcionalidad de auto ejecutar cualquier aplicación o instalación de controladores de dispositivos desde un medio externo.

23. Recomendamos tener un modelo de encriptación que impide su reproducción en otros escenarios.

Respuesta:
Actualmente la información de la memoria USB esta encriptada.

24. Se recomienda estampar las memorias porque son genéricas para una mejor identificación.

Respuesta:

Las memorias utilizadas son todas de las misma marca, modelo y tamaño por cuanto pueden ser identificadas fácilmente. Su tamaño discreto es una de las ventajas observadas para su utilización, sin embargo, hacen difícil su identificación con alguna estampa. Las memorias fueron adquiridas en el proceso electoral del 2016.

25. Recomendamos un procedimiento para enrolamiento de las memorias con las terminales.

Respuesta:

Es importante resaltar que las memorias USB no hacen lectura ni es permitida la ejecución de programas fuera de los autorizados.

Esta recomendación es de procedimiento y de bajo impacto. La misma será evaluada para ser incorporada a futuras versiones.

26. **Se recomienda emitir anexos de erratas cuando sea modificado alguno de los pasos en el instructivo, para asegurar el cumplimiento de las responsabilidades de los miembros de la mesa de votación.**

Respuesta:
En los reforzamientos de los entrenamientos para los miembros de las mesas y los técnicos informáticos fueron actualizadas todas las informaciones relevantes al proceso. El procedimiento habitual de surgir algún imprevisto es informarlos mediante circulares previamente autorizadas.

27. **Se recomienda trabajar en un procedimiento para el control de cambio de las versiones del aplicativo vitales en el proceso.**

Respuesta:
Con relación al voto automatizado estamos usando la estructura de control de versión vía GITLAB. Se complementan con el uso de tres servidores para mantener una separación entre el desarrollo, la calidad y la producción.

Ver. Gitlab.com

28. **Se recomienda solicitar garantías firmadas de seguridad y monitoreo de los servicios entregados por los proveedores CLARO y ALTICE, previo-durante-posterior a la jornada.**

29. **Se recomienda tener un procedimiento para auditar a las telefónicas en materia de seguridad de la información que se estará transmitiendo por dichas plataformas.**

Respuesta 28 & 29:

La JCE tiene comprendido visitar los centros de monitoreo de las telefónicas para todos los procedimientos electorales. Específicamente para las primarias del 6 de octubre 2019, las visitas están pautadas para los días 2 y 3 de octubre. Los funcionarios de las instituciones en base al acuerdo de servicios adquiridos por la JCE hacen presentaciones de los controles y medidas de seguridad que ellos poseen.

La Policía militar Electoral trabaja en coordinación con los proveedores establecen los procedimientos de protección de los puntos claves.

2

Procedimiento Sustitución Equipos Módulo de Votación Automatizada Elecciones Primarias 2019

INTRODUCCIÓN

La dirección de Informática con miras a la celebración de la Elecciones Primarias de los Partidos Políticos 2019, ha procedido a la elaboración de procedimientos que, para garantizar el funcionamiento y efectividad del Sistema del Módulo de Votación Automatizada, en todas sus vertientes, aplicando las misma bajo las normas requeridas dando cumplimento y aplicando las mejores prácticas.

OBJETIVO GENERAL

Validar que la solicitud de cambio cumpla con el procedimiento establecido, para ejecutar acción sin que esta afecta o ponga en tela de juicio la credibilidad del proceso electoral.

ALCANCE

Todos los equipos que componen el módulo de Votación Automatizado a utilizar en proceso de elecciones Primarias de los Partidos Políticos 2019.

Procedimiento para sustitución de los equipos del Módulo de Votación Automatizado, una vez iniciado el Proceso Electoral

Equipos Genéricos (Monitor, Mini Laptop, Impresora, Lector QR, Fuentes, Memorias USB, Modem 3g, Cables e Inversor)

Una vez iniciado el proceso de votación y durante el mismo si se presentan incidencias con algunos de los equipos se procederá a:

1. Verificar la necesidad de cambio.
2. Generar la incidencia vía Help-desk Electoral
3. Help-desk Electoral crea el reporte de incidencia, indica al Soporte Técnico de Recinto el protocolo a seguir y le da seguimiento al reporte hasta concluir.
4. El soporte Técnico de Recinto procede a comunicarse con el Supervisor Técnico del Recinto para que el mismo reevalúe la incidencia reportada y de proceder entregar el equipo solicitado.
5. El Soporte Técnico de Recinto procede a realizar la sustitución del equipo y ejecutar las pruebas de lugar para confirmar el correcto funcionamiento del equipo, una vez realizado completa el check list o lista de comprobación de solicitud de cambio elaborado para los fines.
6. Una vez concluida la instalación se reinicia el proceso de votación.
7. El Soporte Técnico de recinto firma el comprobante de solicitud de Cambio de Equipo como recibido conforme. (ver anexo pag.5)

Urna de Votación (Mini CPU)

1. Verificar la necesidad de cambio.
2. Generar la incidencia vía Help-desk Electoral
3. Help-desk Electoral crea el reporte de incidencia, indica al Soporte Técnico de Recinto el protocolo a seguir y le da seguimiento al reporte hasta que este concluye.
4. El soporte Técnico de Recinto procede a comunicarse con el Supervisor Técnico para que el mismo reevalúe la incidencia y de proceder este, autoriza la sustitución.
5. De ser aprobada la solicitud se procede a inactivar el ID de la mesa y se autoriza la urna nueva suministrando el ID de la misma para que proceda la autorización.
6. Una vez autorizada la sustitución del equipo, el supervisor técnico hace entrega del CPU al Soporte Técnico de Recinto, el cual procede a realizar la instalación, restaurar la urna de votación y confirmar el correcto funcionamiento del equipo sustituido.
7. Una vez concluida la instalación se reinicia el proceso de votación.
8. El Soporte Técnico de recinto firma el comprobante de solicitud de Cambio de Equipo como recibido conforme. (ver anexo pag.5)

Validación de Técnicos para autorización de sustitución de Urna de Votación.

Confirmar que el soporte técnico que solicita la sustitución del equipo, sea la persona acreditada con el número de credencial único suministrado por la Junta Electoral al momento de ser designado como soporte técnico en una demarcación determinada según se muestra imagen adjunto.

De no confirmase la veracidad de la información suministrada, el operador del seguimiento y monitoreo de incidencias electorales, procederá a contactar al supervisor técnico de la demarcación de la cual se está reportando la incidencia.

Anexo.

Formulario de cambio.

Junta Central Electoral
Dirección de Informática

SOLICITUD CAMBIO DE EQUIPO

Fecha de la solicitud: _____ Hora: _____

Municipio: _____

Recinto: _____ Mesa: _____

EQUIPO	CODIGO
Monitor	○
MiniCPU HP	○
USB de backup	○
Impresora HP	○
Modem 3G	○
Laptop HP	○
Lector QR	○
Inversor	○
Otros	○

Razón de sustitución: _____