Organización de los
Estados Americanos

Secretaría de Asuntos Políticos (SAP)
Departamento para la Cooperación y Observación Electoral (DECO)
Misión de Observación Electoral
Elecciones Generales, Honduras 2013

Informe Final

Auditoría para la verificación de la calidad y transparencia en el funcionamiento del sistema integrado de escrutinio y divulgación electoral (SIEDE) implementado por el Tribunal Supremo Electoral de Honduras para las elecciones generales del 24 de noviembre de 2013.

Tegucigalpa, 20 de noviembre de 2013

INDICE

Resumen Ejecutivo

El siguiente informe presenta los resultados, hallazgos y recomendaciones de la auditoría realizada por la OEA al Sistema Integrado de Escrutinio y Divulgación Electoral (SIEDE) implementado por el Tribunal Supremo Electoral (TSE) de Honduras para las elecciones generales del 24 de noviembre de 2013.

Esta auditoría, realizada a solicitud del TSE, se enmarca dentro del "*Compromiso de garantías mínimas para la ética y la transparencia electoral*" suscrito por el Tribunal y los nueve partidos políticos que participan en el actual proceso electoral. El objetivo principal es verificar la calidad y transparencia del nuevo sistema de transmisión de resultados, circunscribiendo su alcance a la factibilidad técnica de los procesos automatizados críticos para su funcionamiento.

Las actividades de la auditoría se desarrollaron entre el 24 de octubre y el 20 de noviembre de 2013, fecha de entrega de este informe. Es importante señalar que tal como se observó durante el desarrollo de las actividades de esta auditoría, los distintos aspectos del proyecto SIEDE han ido evolucionando y corrigiendo asuntos críticos, por lo que las conclusiones se restringen al estado del sistema hasta el día 16 de noviembre de 2013, fecha en que se realizó el último simulacro al sistema por parte del TSE. Existe, por tanto, la posibilidad que recomendaciones vertidas en el presente documento hayan sido implementadas con posterioridad y que el proyecto continúe experimentando adecuaciones y mejoras previo al día a las elecciones.

Tal como se encuentra estipulado en el plan operativo que define el alcance y objetivos de esta auditoría, las conclusiones expuestas en este documento son el resultado del análisis de los componentes del SIEDE basados en el relevamiento y convalidación de información relacionada al desarrollo funcional del sistema.

Los hallazgos se refieren fundamentalmente al comportamiento del sistema durante los simulacros, lo cuales se llevaron a cabo sin la totalidad de las funcionalidades previstas y con cargas de prueba inferiores a los objetivos definidos para esta auditoría. Por este motivo, las conclusiones se refieren al comportamiento del sistema hasta las fechas mencionadas sin posibilidad de predecir su desempeño con volúmenes de información y carga esperados el día de los comicios.

En términos generales, y bajo las condiciones técnicas de funcionamiento observado, los módulos operacionales que integran el sistema en su conjunto son funcionales, cumpliendo con los parámetros establecidos dentro del proceso del SIEDE. Sin embargo, producto de las brechas existentes entre las pruebas de carga logradas durante los simulacros, y la información que el sistema deberá procesar el día de la elección, el área de consolidación e integración y divulgación de datos presenta una especial preocupación, toda vez que se observó un bajo desempeño en los sistemas de cálculo de acumulación de resultados y adjudicación de cargos. Por

ello resulta prioritario optimizar los mecanismos utilizados en el procesamiento de la información y concluir con las tareas de verificación.

Calidad

En relación a la evaluación de la calidad del SIEDE, es necesario mencionar que la ausencia de manuales de requerimientos constituye un impedimento para el análisis del proyecto en base a métricas de cumplimiento de estándares.

Como se explicita en detalle en el informe, la seguridad del sistema tiene un impacto transversal a las distintas funcionalidades del SIEDE. En este sentido, retrasos en el aprovisionamiento de productos informáticos para completar la infraestructura de seguridad y una planificación tardía de estos módulos ha redundado en la existencia de vulnerabilidades que requieren de inmediata atención por parte del TSE.

En relación a la calidad del software, la auditoría analizó la corrección, fiabilidad, eficiencia, integridad y facilidad de uso, que en su conjunto constituyen elementos de buenas prácticas internacionales para el desarrollo de programas.

Los módulos que comprenden el tratamiento de actas, incluyendo el escaneo, impresión y transmisión, recepción de actas digitalizadas, retransmisión a partidos políticos y auditoría internacional, análisis de consistencia de las actas transmitidas, transcripción, verificación de actas y monitoreo de inconsistencias cumplen con los estándares de calidad requeridos para este proceso en particular. Se conservó la integridad de los datos transmitidos mientras que los resultados obtenidos y entregados a las siguientes etapas fueron correctos.

En relación al módulo de consolidación, integración y divulgación de los resultados la auditoría detectó fallas que evidenciaron el no cumplimiento con estándares de calidad requeridos para este tipo de programas. Es importante destacar que aspectos como corrección, fiabilidad y eficiencia no han sido cumplidos por estos módulos hasta la finalización de los simulacros.

En lo referente a la divulgación de los resultados, la auditoría pudo evidenciar problemas que obligaron a un rediseño de la aplicación. Por dicho motivo a la fecha no ha sido posible realizar un análisis de vulnerabilidades toda vez que no se cuenta con una versión definitiva del programa.

Transparencia

En relación a la transparencia, la auditoría desea destacar que el sistema, desde un punto de vista de su funcionalidad, constituye en su conjunto un importante avance en garantizar el acceso a la información tanto a los partidos políticos, a la Auditoría Internacional y a la ciudadanía en general.

El manejo secuencial de la información, desde que el acta es escaneada y transmitida, pasando por su retransmisión a los partidos políticos hasta su divulgación definitiva en caso de consistencias en las información, permitirá a los distintos actores del proceso electoral ir conociendo los resultados bajo criterios de ordenamiento de cola sin intervención de factores adicionales, ofreciendo garantías de transparencia y equidad en la entrega de la información.

Del mismo modo, los módulos encargados de la digitación y validación de las actas mediante sistemas de revisión ciego, con verificación cruzada y capas de validación en casos de inconsistencias, cumple con garantizar un manejo de los datos de manera transparente, respetando las preferencias de la ciudadanía durante el proceso electoral.

La auditoría desea agradecer al TSE por la confianza depositada en la OEA para realizar este trabajo. Del mismo modo, desea reconocer y agradecer el apoyo financiero que los Estados Miembros y Observadores Permanentes otorgan a las actividades de Observación Electoral dentro de las cuales se enmarcó este trabajo.

Introducción

Las Misiones de Observación Electoral buscan contribuir al mejoramiento de los procesos y sistemas electorales por vía de sus recomendaciones, que pueden servir de hoja de ruta para los actores clave sobre qué elementos de sus procesos se pueden mejorar. En el marco de previas MOEs/OEA a Honduras, se tomó nota de los retos asociados con una transmisión preliminar de resultados a voz y se recomendó, en aras de modernizar el proceso y agregarle aún más elementos de transparencia, la transición a un sistema de transmisión de resultados por vía electrónica.

En el marco de los preparativos para el desarrollo de las elecciones generales del 24 de noviembre de 2013 en Honduras, el Tribunal Supremo Electoral (TSE) tomó la decisión de implementar esta recomendación, e inició los preparativos para poner en práctica el Sistema Integrado de Escrutinio y Divulgación Electoral (SIEDE). Adicionalmente, esta medida fue uno de los elementos del "*Compromiso de garantías mínimas para la ética y la transparencia electoral*" suscrito en agosto 22 del 2013 entre el TSE y los nueve partidos políticos que participan en el actual proceso electoral. Ese documento estipula que se solicitaría a una entidad internacional una auditoría del sistema de transmisión de resultados. En este sentido, mediante nota fechada del 22 de octubre, el TSE solicitó a la Organización de los Estados Americanos el desarrollo de una auditoría internacional al sistema.

Dentro de los objetivos principales de las Misiones de Observación Electoral de la OEA (MOEs/OEA) se encuentra el colaborar con las autoridades gubernamentales y electorales, y con la ciudadanía en general, para asegurar la imparcialidad, transparencia y confiabilidad de los procesos electorales; contribuir a crear una atmósfera de confianza pública y alentar la participación de la ciudadanía así como formular recomendaciones con el fin de contribuir al mejoramiento del sistema electoral. Este trabajo de revisión del SIEDE busca entonces cumplir con estos objetivos de las Misiones de Observación Electoral de la OEA.

La auditoría, que se enmarca dentro del "*Compromiso de garantías mínimas para la ética y la transparencia electoral*" , tuvo como objetivo principal, verificar la calidad y la transparencia del nuevo sistema de transmisión de resultados. Su alcance se restringió al análisis de la factibilidad técnica de los procesos automatizados críticos para el éxito del mismo.

Con la llegada a Honduras de un equipo integrado por dos auditores informáticos y un grupo de especialistas en tecnología electoral y en observación de procesos electorales, la auditoría inició sus actividades el 24 de octubre de 2013 con la elaboración de un plan operativo de trabajo y finalizó el día 20 de noviembre de 2013, con la entrega de este informe.

El presente documento tiene por objeto presentar los hallazgos y conclusiones de la auditoría al Sistema Integrado de Escrutinio y Divulgación Electoral (SIEDE). En la primera sección, se entregan detalles del alcance de la auditoría y la metodología

implementada en el marco de este proyecto. La segunda sección contiene información respecto al desarrollo y resultados finales de los tres simulacros desarrollados por el TSE al SIEDE. En la tercera sección se entrega información sobre los hallazgos generales de la auditoría al sistema en cada una de sus etapas, agrupadas de acuerdo a su funcionalidad. Debido a su tratamiento transversal a las diferentes áreas del SIEDE se analiza, bajo un cuarto capítulo, la seguridad informática del sistema. Finalmente, la quinta sección entrega las conclusiones finales de la auditoría.

La Misión de Observación Electoral de la OEA desea agradecer al TSE la confianza puesta en la Organización para colaborar en esta revisión del SIEDE y contribuir así a un mejoramiento del sistema de transmisión de resultados. Del mismo modo, desea reconocer y agradecer el apoyo financiero que los Estados Miembros y Observadores Permanentes otorgan a las actividades de Observación Electoral dentro de las cuales se enmarcó este trabajo.

I. Alcance y Metodología

Alcance

El alcance de la auditoría se enmarcó estrictamente en la factibilidad técnica de los procesos automatizados críticos para el éxito del SIEDE a fin de constatar si reúne condiciones mínimas de calidad y transparencia.

Para efectos de esta auditoría, se precisaron los componentes asociados con la calidad y transparencia del sistema de la siguiente forma:

- Calidad: Cumplimiento del SIEDE con estándares internacionales de programación de los diferentes módulos del software, incluyendo seguridad informática, y su cumplimiento con los requerimientos pre-establecidos por el TSE para su funcionamiento.
- Transparencia: verificación de las facilidades y garantías brindadas a los diferentes actores políticos y ciudadanos para la constatación del funcionamiento del sistema el día de la votación.

En relación a los procesos contemplados dentro del alcance de esta auditoría, se establecieron cuatro etapas agrupadas de acuerdo a su funcionalidad:

a. Escaneo, impresión y transmisión de actas desde los centros de votación,
b. Recepción de actas digitalizadas, retransmisión de actas a partidos políticos y a la Auditoría Internacional y análisis de consistencia de las actas transmitidas,
c. Transcripción y verificación de actas, y monitoreo de inconsistencias
d. Consolidación e integración de los datos cargados y divulgación de resultados.

En relación al hardware, se consideró dentro de esta auditoría aquella infraestructura tecnológica empleada en las funcionalidades mencionadas arriba, poniendo especial énfasis en los aspectos de seguridad y funcionamiento continuo del servicio.

En relación a la infraestructura en telecomunicaciones, se consideraron los siguientes segmentos de transmisión de datos que vinculan sistemas de información y/o módulos:

- Entre los Centros de Transmisión (ATX) y la recepción de imágenes de actas en el Centro de Procesamiento del TSE;
- Entre el escrutinio especial y el SIEDE;
- Entre el SIEDE y la divulgación de resultados;

- Entre el SIEDE y la Auditoría Internacional[1].

Para efectos de esta auditoría, se consideró a la seguridad como un elemento transversal al software, hardware e infraestructura de telecomunicaciones por ello será analizado bajo una sección independiente en este informe.

Cabe mencionar, que esta auditoría no contempló aquellos módulos o programas, infraestructura de hardware y telecomunicaciones que son complementarios al SIEDE o que no fueron desarrollados bajo la dirección, verificación, intervención y supervisión directa del TSE incluyendo: las funcionalidades asignadas a la Auditoría Internacional, las funcionalidades relacionadas con la salida y retorno de maletas electorales, recepción y escaneo de actas al momento de recibir las maletas electorales, de escrutinio especial y, de escaneo de los cuadernos de votación. Se excluyen además, aquellos procesos o sistemas que son distintos a los involucrados en el SIEDE y cuyo uso es con posterioridad al acto electoral, con excepción de los servicios contratados por éste para el día de los comicios como el caso de los enlaces que dispondrán las empresas TIGO y CLARO.

Consideraciones preliminares

Con la finalidad de recrear condiciones de funcionamiento semejantes a la tensión de trabajo y prueba de esfuerzo esperada al momento de los comicios de fecha 24 de noviembre, la auditoría previó condiciones mínimas que debían cumplir los tres simulacros planificados por el TSE llevados a cabo los días 8, 15 y 16 de noviembre de 2013.

Al respecto, el plan operativo firmado entre la MOE/OEA y el TSE, y que define los lineamientos y alcances de la auditoría, requirió la implementación de un mínimo del 100% de funcionalidad del sistema durante los simulacros, a fin de (a) evaluar la efectividad de los componentes, (b) se produjesen hallazgos relevantes y (c) se brindasen recomendaciones en base a la verificación del sistema en funcionamiento. Cabe anotar que un 100% de funcionalidad se refiere a poder contar con y revisar, en el marco de la auditoría el hardware y software en su versión final.

Adicionalmente, se estableció en el plan operativo el requerimiento que se transmitiesen en los simulacros a ser observados al menos un 80% del volumen de las actas por cada nivel electivo, distribuidas en la totalidad de Centros de Transmisión. Esto era imprescindible a fin de evaluar el funcionamiento del sistema con una tensión de trabajo bastante próximo al día de la elección, y contemplando

[1] La Auditoría Internacional, como institución independiente al TSE, posee su centro de procesamiento en un inmueble físicamente distinto al dispuesto por el TSE para el SIEDE. Cabe resaltar que esta auditoría no cubrirá una evaluación de aquellos procesos que el TSE ha asignado a esta entidad por caer fuera del ámbito dirección, verificación, intervención y supervisión directa del TSE.

las diversas posibilidades que se pudiesen presentar durante el llenado de las actas de cierre y el manejo de las mismas por el SIEDE.

Metodología y Equipo de trabajo

El análisis realizado comprendió el relevamiento y convalidación de información relacionada al desarrollo funcional del sistema así como la observación de los tres simulacros desarrollados por el TSE a fin de constatar las condiciones mínimas de calidad y transparencia.

Las actividades de esta auditoría se llevaron a cabo siguiendo los lineamientos establecidos en el plan operativo firmado entre la MOE/OEA y el TSE (ver anexo requerimientos del plan operativo) comprendiendo:

- Análisis de los procesos automatizados en las diferentes etapas que componen el SIEDE.
- Revisión y análisis de los componentes críticos para el éxito del sistema de software definidos por esta auditoría, a fin de corroborar que cumpla con los casos de uso.
- Revisión y análisis de procesos relacionados que puedan representar potenciales riesgos al SIEDE.
- Lectura y análisis de diagramas y documentos recopilados durante el relevamiento.
- Documentación del relevamiento a través del uso de narrativos y comparación entre lo relevado, constatado y en funcionamiento.
- Revisión del hardware de telecomunicaciones y procesamiento, con el fin de determinar si es acorde a la función que debe desempeñar, en condiciones similares a las del día de las elecciones, y asegurar la transmisión y almacenamiento de los datos de manera segura.
- Evaluación del ambiente de control interno y de los controles generales de tecnología informática, tales como seguridad física y lógica.
- Análisis de las políticas, manuales, procedimientos escritos y los esquemas de seguridad dispuestos en las distintas etapas del proyecto SIEDE, con la finalidad de garantizar la seguridad de los datos.
- Análisis de los esquemas de seguridad de acceso a los datos por parte de los usuarios y operadores, así como también accesos no autorizados.
- Revisión de código fuente e interfaces de los sistemas de Transmisión de Actas desde los Centros de Votación, Monitoreo de Inconsistencias y Consolidación e Integración de los datos cargados y Divulgación de resultados.
- Revisión de los planes de contingencia para el día de la elección relacionados al SIEDE.
- Evaluación de la existencia y actualización de los manuales de usuarios y técnicos de los sistemas intervinientes.
- Ejecución de pruebas de validación de datos de entrada de los sistemas intervinientes, en ambiente de prueba.

- Evaluación de los resultados obtenidos y documentación de los hallazgos de auditoría.

El equipo de auditoría de la MOE/OEA estuvo integrado por cinco profesionales a cargo de llevar a cabo el relevamiento y análisis de la información que hace parte de este informe:

Tabla 1. Equipo Auditor OEA

Nombre	**Nacionalidad**	**Equipo**
Arsenio Cardona	Argentino	Auditor - Perito informático
Héctor Hernández	Argentino	Auditor - Perito informático
Adriana Parcerisa	Paraguaya	Especialista en tecnología electoral
Gustavo Aldana	Guatemalteco	Especialista en tecnología electoral
David Álvarez Veloso	Chileno	Especialista electoral OEA

II.- Simulacros en Cifras

Los simulacros realizados al SIEDE se desarrollaron los días 8, 15 y 16 de noviembre de 2013. La auditoría observó y evaluó las condiciones generales de desempeño del sistema en cuando a su calidad, seguridad y transparencia así como su funcionalidad.

De acuerdo a los datos proporcionados por el TSE, las siguientes son las cifras oficiales respecto del total de centros de votación, y transmisión de actas que fueron parte de los tres simulacros del SIEDE.

Tabla 2. Cifras de los Simulacros SIEDE: Centros de Votación

Categoría	Simulacro 8 de Noviembre	Simulacro 15 de Noviembre	Simulacro 16 de Noviembre
Centros de Votación	5.754	5.754	5.754
Centros de Votación SIEDE (con señal)	5.143	5.143	5.143
Centros con Kit Tecnológico	1.721	2.083	2.083

Fuente: Elaboración OEA para este informe con datos TSE.

Tabla 3. Datos de los Simulacros SIEDE: Transmisión de Actas

Categoría	Simulacro 8 de Noviembre	Simulacro 15 de Noviembre	Simulacro 16 de Noviembre
Cantidad Total de Actas país	48.282	48.282	48.282
Cantidad de Actas Distribuidas	31.431	25.203	25.203
Actas Transmitidas	7.949	17.256	19.536
Actas transmitidas con firma digital válida	7.942	Sin información a la fecha de este informe	Sin información a la fecha de este informe
Actas transmitidas con firma digital inválida	7	Sin información a la fecha de este informe	Sin información a la fecha de este informe

Fuente: Elaboración OEA para este informe con datos TSE.

Tabla 4. Esquema de distribución porcentual de los datos correspondientes a los tres simulacros

	Simulacro 8 de Noviembre	**Simulacro 15 de Noviembre**	**Simulacro 16 de noviembre**
Total de Kits a Distribuir	5.092	5.092	5.092
Total de Centros de Votación	5.754	5.754	5.754
Centros de Votación SIEDE (con señal)	5.143	5.143	5.143
Cantidad de Centros con Kit Tecnológico	1.721	2.083	2.083
Proporción de Centros de Votación con Kit	33%	41%	41%
Cantidad de MER	10.477	8.401	8.401
Cantidad de Kits Distribuidos	1.987	2.181	2.181
Proporción de Kit distribuidos	39%	43%	43%
Cantidad de Kits Distribuidos	1.987	2.181	2.181
Cantidad de Kits en Línea	628	1.705	1.994
Proporción de Kits Tecnológicos en Línea del total distribuido	32%	78%	91%
Proporción de Kits en línea del total a distribuir	12.33%	33.48%	39.15
Cantidad de Actas Distribuidas	31.431	25.203	25.203
Proporción de Actas Distribuidas	65%	52%	52%
Cantidad de Actas Transmitidas	7.949	17.256	19.536
Cantidad Total de Actas	48.282	48.282	48.282
Proporción de Actas Transmitidas respecto a las Distribuidas	25%	68%	78%
Proporción de Actas Transmitidas respecto del Total de Actas a transmitir el día de la elección	16.46%	35.74%	40.46%

Fuente: Elaboración OEA para este informe con datos TSE.

III. Hallazgos de la auditoría

A continuación se presenta el análisis de las etapas evaluadas por esta auditoría. Para ver en detalle del comportamiento de cada una de las dimensiones contempladas, se adjunta en cada sección una tabla sintetizando los hallazgos y recomendaciones.

A.- Escaneo, impresión y transmisión de actas desde los centros de votación

Considerando que durante los simulacros el desempeño de esta funcionalidad en su conjunto (notebook, impresora/scanner y enlace) operó con carga de trabajo del 40.46% respecto del caudal esperado para el día de los comicios, la auditoría no cuenta con información suficiente para evaluar el comportamiento potencial de la infraestructura de telecomunicaciones para el día de la elección. Sin embargo, los siguientes son los hallazgos respecto del comportamiento del sistema en base a los simulacros.

De acuerdo a las especificaciones técnicas del SIEDE, el kit tecnológico o ATX está conformado por una impresora multifuncional, un notebook y un modem. Durante el desarrollo de los simulacros, la auditoría pudo observar algunos problemas técnicos, principalmente con el desempeño inadecuado de algunas impresoras, situación que en general pudo ser corregida tras las sucesivas pruebas del sistema.

En relación a la operación de los ATX, la auditoría pudo detectar problemas de trasmisión de actas durante el simulacro debido a inconvenientes en la asignación de contraseñas a los operadores de estos ATX. Durante los consecutivos simulacros, la auditoría pudo constatar que la entrega de información de usuario y contraseña, vía mesa de ayuda telefónica, permitió la operación adecuada del sistema, no constatando inconvenientes en las funcionalidades del software y conexión de datos.

A través del análisis de esta funcionalidad, la auditoría pudo constatar algunas debilidades emanadas de las pruebas y evaluaciones específicas de los módulos establecidos en el Plan Operativo, incluyendo:

- Falta de un método de control de versión de software en los ATX que permita garantizar de manera comprobable y verificable el uso de una misma versión del software en todo los kits.
- Problemas de sincronización de la fecha y hora de los ATX con los servidores que puede impedir el análisis posterior de logs.
- El envío de archivos hacia los partidos políticos y Auditoría Internacional previa validación de firma digital, tal como fue solicitado por los propios partidos tiene

como consecuencia el exponer el sistema a la transmisión de archivos defectuosos, incorrectos o incompletos (propios de una transmisión no validada). En este tipo de procesos siempre la transmisión de datos hacia servidores de visualización debe incluir una validación previa de la información a suministrar. Por último, no existe razón técnica que justifique la exclusión de dicho control de integridad. Al contrario su uso puede contribuir a la seguridad de los datos que procesa el sistema.

- La falta de un adecuado licenciamiento del sistema operativo de las notebook que conforman el kit tecnológico a ser utilizado en los ATX expone a la infraestructura de no disponer de las actualizaciones correspondientes al sistema operativo.
- Falta de implementación de una cadena de custodia y seguimiento de los kits tecnológicos en el proceso de despliegue y entrega, desde que salen de la bodega tecnológica nacional, hasta que lleguen a los centros de votación y sean finalmente dispuestos a los operadores de los ATX que garanticen la inalterabilidad del hardware y del software.
- Falta de documentación adecuada de procesos en manuales o protocolos de operación.

Por su parte, esta funcionalidad en su conjunto presenta fortalezas en materia de transmisión, dadas tanto por el uso de un canal seguro, como por el envío secuencial de las actas, lo que garantiza su procesamiento de acuerdo al orden de llegada de las mismas.

En cuanto a condiciones técnicas de funcionamiento, el Kit Tecnológico en su conjunto es funcional, cumpliendo con los parámetros establecidos dentro del proceso del SIEDE. El análisis no permite, sin embargo, predecir el desempeño del sistema con el caudal esperado para el día de los comicios.

Tabla 5. Escaneo, impresión y transmisión de actas desde los centros de votación: Resumen de hallazgos de la funcionalidad

Proceso evaluado de acuerdo al Plan operativo[2]	Cumple los requisitos	Desempeño / observaciones	Recomendaciones / observación
8.2.a	Si	Prueba realizada. Resultado favorable, la totalidad de la infraestructura eléctrica instalada en el Hotel plaza Juan Carlos, fue soportada por un equipo electrógeno sin alterar el funcionamiento.	
Enlace de datos entre los ATX's y	Si	Nivel de operatividad menor al previsto. Ver cifras en tabla 4.	

[2] Para detalle de los procesos en todas las tablas ver anexo 1.

el SIEDE			
3.a	No	Falta de un mecanismo de control de versión del programa que utilizan los ATX's que permita conocer si la versión instalada es la última y se aplica en todos.	Modificar e implementar los cambios necesarios que permitan constatar que todos los ATX cuentan con la misma versión de programa. Se propone un mecanismo de cálculo de hash del/los programa/s y la correspondiente documentación.
3.b	No	El ATX permite la transmisión de imágenes almacenadas en él, sin encontrarse usuario alguno conectado al APN.	Impedir que se transmita de manera automática sin haberse autenticado el usuario de la ATX.
	No	En relación a los logs que envían los ATX's al momento del cierre, se observa que se almacenan en el disco rígido del ATX y viajan por un canal seguro pero sin mecanismo de encriptación alguno.	Encriptar los logs en el disco rígido del ATX y enviarlo del mismo modo al servidor central al momento de cerrar el ATX como mecanismo extra de seguridad (canal seguro).
3.d	No	Valor de fecha y hora en el ATX no sincronizada con servidores, lo que impide efectuar un adecuado seguimiento de los eventos.	Es necesario mantener una fuente de tiempo uniforme y confiable, tanto para los ATX, como para los servidores y computadoras relacionadas al proyecto SIEDE.
3.d	No	Los logs que se almacenan en los ATX son de texto plano, lo que permite su acceso de manera directa al contenido.	Utilizar un algoritmo de encriptación en los logs.
3.e	Si	Se ha construido una red APN entre los ATX y el Centro de Procesamiento dispuesto por el TSE. En ese canal se aplica HTTPS combinado con el protocolo SSL. Por otro lado, la imagen escaneada se almacena en un archivo XML con clave de cifrado, y contempla la integridad con firma digital. Cumple el requisito prefijado.	
3.f	Si	Analizando las funcionalidades del sistema desde la transmisión de las actas de los ATX, pasando por las distintas etapas, hasta la Divulgación de resultados, se observa que las mismas fluyen por el sistema según el estado en	

		el que se encuentre, de manera secuencial y no bajo un criterio de ordenamiento.	
3.h	Si	Ante inconvenientes en la autenticación del operador del ATX durante el primer simulacro, el operador no sabía dónde consultar. Se observó satisfactoriamente en los siguientes simulacros que el operador contactaba a la mesa de ayuda ante cualquier inconveniente.	El procedimiento respondió de acuerdo a lo esperado.
3.i	Si	Del análisis funcional que se efectuó desde la transmisión de las actas desde los ATX, siendo receptadas y sin validación de firma digital se retransmite a nueve servidores y un servidor adicional, dispuestos por el TSE, para nueve partidos políticos y Auditoría Internacional, respectivamente	Los partidos políticos cuentan con acceso a los archivos transmitidos desde los ATX en los servidores dispuestos por el TSE. Respecto a Auditoría Internacional, la misma dispone de los archivos transmitidos por cada ATX y enlace de datos, faltando que la empresa MAPA construya las API específicas que permiten interactuar con los datos del SIEDE.
3.j	No	Por la trascendencia del evento, por un lado, y por la seguridad de la infraestructura tecnológica, por el otro, es necesario disponer del licenciamiento del sistema operativo correspondiente. En cuanto al aspecto de seguridad, se refiere a las actualizaciones y parches que deben instalarse. Este aspecto afecta a todo el parque tecnológico que participa en el proyecto, o sea, ATX, computadoras y servidores.	Acreditar fehacientemente la modalidad de licenciamiento aplicada a los equipos ATX, computadoras y servidores.
3.k	No	La clave del usuario “Administrador” de los ATX es conocida por técnicos de la empresa MAPA, no así por personal del TSE. El traspaso de claves al TSE se efectuará una vez consolidada la última versión del sistema de los ATX. Debiendo los técnicos del TSE solicitar se coloque la clave para efectuar pruebas.	Establecer un mecanismo formal de administración y traspasos de claves hacia el TSE.

4.a	No	En relación al almacenamiento de los Kit Tecnológicos, no se observa la presencia de mecanismos que impidan el acceso directo al contenido, ni señale los responsables de su manipulación y operación.	Establecer e instrumentar un mecanismo de cadena de custodia y preservación, basado en precintos y fichas con responsables para su manipulación (apertura, operación y embalaje).
6.d	No	Al momento de la puesta en cero de los datos de los ATX, el proceso también borra el contenido de uno de los archivos de log que se usa para ese proceso.	Revisar y corregir el proceso de puesta a cero y aplicarlo en todos los ATX.
6.e	No	Conocer el mecanismo que detenga el funcionamiento de las bases de datos dispuestas para el Proyecto SIEDE, después de haber finalizado el Primer Turno de Transcripción, a las 03:00 horas del 25 de noviembre de 2013, con la finalidad de obtener los respaldos correspondientes.	Documentar y formalizar el método a utilizar para el cierre de la actividad electoral.
Inventario de Hardware	No	Modems perdidos o sustraídos de las empresas TIGO y CLARO, posibilitaría escalar privilegios en la red APN.	Identificar e individualizar esos módems, y solicitar a las empresas CLARO y TIGO, la deshabilitación de los mismos a través del número de línea, IMSI o Tarjeta SIM.
	No	Actualmente se corre el riesgo de que ante la pérdida de un notebook, pueda ser deducida la clave del usuario administrador del sistema operativo.	Cambiar clave de setup y del usuario Administrador de la totalidad de los Kits al regreso de los simulacros.

B. Recepción de actas digitalizadas, retransmisión de actas a partidos políticos, a Auditoría Internacional y análisis de consistencia de las actas transmitidas.

La infraestructura de telecomunicaciones montada en el centro de procesamiento es la responsable de recibir todas las actas que envían los ATX distribuidos por el país. Un conjunto de servidores son los responsables de canalizar los archivos hacia una bifurcación en la cual, en primera instancia, replican los archivos -sin efectuar análisis sobre los mismos- hacia los partidos políticos y Auditoría Internacional y en segunda instancia, entran al proceso de validación por parte del TSE.

Una vez entradas a este proceso de validación, otros servidores son los encargados de analizar la integridad de la firma digital de los archivos para poder ser aceptados en el siguiente proceso. Se extraen las imágenes contenidas de cada archivo de las actas, se envía a publicación en internet el acta con firma digital válida (Módulo no implementado hasta el desarrollo de la auditoría), y un software específico analiza y procesa cada imagen, para poder atomizarla en trozos pequeños, y de tal manera, poder presentarlos a los transcriptores de manera aleatoria sin permitir ver datos correspondientes a partidos políticos y candidatos

Es importante señalar que el desempeño de la funcionalidad de "recepción de actas digitalizadas, retransmisión de actas a partidos políticos, a Auditoría Internacional y análisis de consistencia de las actas transmitidas" fue de un 78% de las actas transmitidas respecto a las actas distribuidas para el último simulacro. Si bien se pudo analizar su operatividad con la carga señalada, no se puede predecir el comportamiento de toda la infraestructura tecnológica con el caudal que se disponga en el día de los comicios.

Del análisis del sistema en su conjunto, y tras observar el desempeño de los simulacros, la auditoría pudo detectar algunos elementos que son sujetos de mejoras para el desarrollo de la elección:

- El software Iris (análisis y segmentación de las imágenes) basa su control de versiones en un sistema informatizado administrado por la empresa proveedora. Pese a ello no se ha podido constatar de qué modo puede la autoridad electoral certificar que la última versión que indica el control de versiones es la utilizada y no ha sido alterada tras su liberación (control de integridad).
- La auditoría pudo constatar que el software específico para el análisis y segmentación de imágenes, posee la licencia de uso correspondiente. No obstante, no se pudo corroborar el licenciamiento en el parque tecnológico que involucra, lo que se trata en el apartado de Seguridad Informática 6.12 Licenciamiento.

Considerando la transparencia del sistema, esta funcionalidad ha sido diseñada para el procesamiento de las actas de acuerdo a un criterio secuencial, en el mismo orden que es recibido. Esto permite poner a disposición de la ciudadanía la información en la medida que se va produciendo, sin ser expuesta a ordenamientos arbitrarios o manipulados. La transmisión de las actas previa validación de firmas digitales hacia

los partidos políticos y Auditoría Internacional, y la divulgación en intranet a los partidos políticos constituye una funcionalidad que aporta en el mismo sentido.

En condiciones técnicas de funcionamiento normal, la infraestructura tecnológica (hardware y software) en su conjunto cumple con las prestaciones requeridas. Pese a lo apuntado, no se pudo corroborar su comportamiento en contingencia debido a que no se halla instalada la respectiva sala de contingencias (infraestructura tecnológica y de telecomunicaciones).

Tabla 6. Recepción de actas digitalizadas, retransmisión de actas a partidos políticos, a la Auditoría Internacional y análisis de consistencia de las actas transmitidas: Resumen de hallazgos de la funcionalidad

Proceso/funcionalidad evaluado de acuerdo al plan operativo	Cumple los requisitos	Desempeño / observaciones	Recomendaciones / observación
Divulgación a la prensa	No	Solo publicado a nivel de intranet.	Montar la infraestructura
Divulgación a los partidos políticos	Si	Divulgación a nivel de intranet.	Funcionalidad cumple con lo esperado y aporta a la transparencia del sistema.
Pruebas de Bases de datos de acuerdo a plan operativo 8.4.a	Si	Prueba realizada con base de datos MSSQL SERVER 2008.	Prueba cumplió con lo estipulado.
Divulgación en internet de acta con firma digital válida.	No	No implementado	Implementar antes de los comicios.

C. Transcripción y verificación de actas, y monitoreo de inconsistencias

Una vez recibidas las actas digitalizadas, y retransmitidas a partidos políticos, a la Auditoría Internacional y analizadas respecto de su consistencia, pasan a la etapa de transcripción, verificación, y monitoreo de inconsistencias. En esta etapa, los operadores instalados en Tegucigalpa verifican visualmente la cantidad de rúbricas contenidas en cada acta, lo que habilita pasar a transcripción o remitir al monitoreo de inconsistencias. Dos grupos de transcriptores digitan los números que visualizan en la pantalla, comparando los valores en el sistema, para posteriormente enviar las actas que presenten inconsistencias a un grupo de verificación. De confirmarse inconsistencias, el acta automáticamente se deriva al escrutinio especial.

Este breve resumen del sistema presenta a nivel general las distintas instancias de esta funcionalidad, destacando su envergadura y complejidad, principalmente dada por la interacción de sus componentes, tanto tecnológicos como humanos.

La fortaleza de esta funcionalidad está dada en su conjunto por el tratamiento secuencial que le otorga a cada acta, a medida que pasa por cada una de las etapas. A favor de la transparencia, no existen criterios distintos a los tiempos de llegada de las mismas que definen su orden de procesamiento. Del mismo modo, la utilización de software que segmenta las imágenes para su transcripción, permite un análisis ciego de las mismas, impidiendo que algún digitador pueda, de manera deliberada, otorgar una votación distinta a candidatos específicos.

Del análisis de la funcionalidad, la auditoría pudo observar debilidades en cuanto a la falta de documentación de protocolos. Por la envergadura de este tipo de proyectos, los manuales y protocolos resultan particularmente importantes toda vez que permiten responder a incidencia e imprevistos de manera adecuada sin depender de operadores específicos.

Tabla 7. Transcripción y verificación de actas, y monitoreo de inconsistencias: Resumen de hallazgos de la funcionalidad

Proceso/funcionalidad evaluado de acuerdo al plan operativo	**Cumple los requisitos**	**Desempeño / observaciones**	**Recomendaciones / observación**
Digitación/Verificación de actas	Si	El proceso no presentó inconvenientes.	Es necesario notar sin embargo, que la carga de trabajo no fue la recomendada por la auditoría.
Monitoreo de Inconsistencias	Si	Desempeño adecuado. Resta verificar los resultados obtenidos cotejando con las actas procesadas.	Concluir con la verificación de la integración del sistema versus la matriz de pruebas.
Probar el ingreso no autorizado de usuarios y corroborar la ejecución de programas no permitidos. 8.5.a	Si	Sistema cumple con lo esperado. No permite el ingreso de usuarios no autorizados. Y el usuario autorizado no tiene permiso para ejecutar otra aplicación.	
3.a	No	Se utiliza un software que le permite llevar un historial de cambios o versión de los cambios que se producen en el E-CORE[3]; no disponiendo fecha cierta para dejar estable la última versión, ni mecanismo de versión.	Fijar fecha límite para no introducir más cambios en el código y aplicar mecanismo de versión.
3.b	No	Se relevó y analizó el Monitor de Inconsistencias, consolidación / integración y	Concluir con la verificación de la integración del

[3] E-CORE es componente que proporciona un entorno de programación.

		divulgación, debiendo comparar los datos del simulacro con los de la prueba controlada.	sistema versus la matriz de pruebas.
3.c	Si	La Divulgación de resultados fue considerada como funcionalidad del sistema.	La Divulgación de resultados se realizó en Intranet, debiendo aún implementarse la publicación en Internet antes de los comicios. En ambos casos resolver inconvenientes en el algoritmo de cálculo y asignación de candidatos, además de concluir y evaluar la última versión del publicador de resultados.
3.k	No	Independientemente del esquema de seguridad instrumentado, se observa que todas estas funcionalidades se encuentran en manos de solo dos personas de MAPA y ningún técnico del TSE; lo que representa un riesgo para la continuidad de los módulos ante la falta de alguno de ellos.	Incorporar de manera urgente un técnico adicional por parte de la empresa MAPA, que domine la tecnología utilizada y los módulos involucrados, ante la imposibilidad de alguno de los técnicos actuales, del mismo modo, por parte del TSE, disponer de un técnico que pueda colaborar para completar y asistir en estos módulos.
4.b	No	Se tomó nota de la falta de diagramación de arquitectura de servidores, distribución de planta y sitios de contingencia, los mismos no están documentados.	Disponer de la documentación de infraestructura y funcionalidad de los módulos, a fin de evitar la dependencia en los actuales operadores.
6.a	No	No se dispone de un diagrama formal de las bases de datos y los servidores involucrados, lo que genera dependencia del personal técnico de la empresa MAPA.	Disponer de la adecuada documentación y el correspondiente entrenamiento de al menos un técnico de la empresa MAPA y otro técnico por parte del TSE.

6.b	No	Se observa la administración de la base de datos a cargo de un solo técnico y la programación a cargo de dos técnicos de la empresa MAPA y ningún técnico del TSE.	Instrumentar un adecuado esquema de trabajo, con la incorporación de al menos un técnico por parte de la empresa MAPA y del TSE que puedan continuar y terminar los sistemas ante la indisponibilidad de alguno de los actuales técnicos.
6.e	No	No se encontró instrumentación formal de cierre y backup.	Diagramar e implementar un mecanismo formal y automático para el momento del cierre de los comicios, que permita dejar registrado los datos al momento del cierre y backup de las bases de datos, sus logs y logs del sistema operativo.

D. Consolidación e integración de los datos cargados, y divulgación de resultados

Esta funcionalidad es la encargada de verificar que los datos cargados por los digitadores o transcriptores estén de acuerdo a los casos de usos estipulados. Aquella acta que no cumpla con las validaciones pasa a escrutinio especial. A través de los procesos de consolidación/integración, se realizan los cálculos para la acumulación de resultados y la adjudicación de cargos tras el escrutinio definitivo. Los datos que se obtienen de estos procesos se utilizan en la divulgación de resultados.

Las fortalezas de esta funcionalidad en su conjunto están dadas por el tratamiento de los datos mediante el uso de colas de tareas de modo secuencial a medida que la información es recibida. El criterio de ordenamiento en este caso se hace sólo en base al orden de llegada de la información, lo cual es un aporte a la transparencia en el manejo de los datos.

Dentro de los aspectos a mejorar detectados en cuanto al software, hardware y datos, de esta funcionalidad se encuentran:

- Durante el desarrollo de los simulacros los procesos de consolidación e integración presentaron un bajo nivel de desempeño, lo que impidió un

oportuno y adecuado cálculo de acumulación de resultados y adjudicación de cargos. Durante el día de los comicios, se espera una carga mayor a la probada en las etapas de simulación, por lo que se considera necesario optimizar los algoritmos de cálculo utilizados para que respondan a la demanda esperada el día de la votación.

- Hasta el término de esta auditoría, no se concluyeron las tareas de verificación de cálculo de acumulación de resultados con respecto a una matriz de carga controlada, acción necesaria para validar los resultados obtenidos por el sistema.

Es importante señalar que los hallazgos de esta funcionalidad constituyen aspectos críticos que deben ser abordados con urgencia antes del desarrollo de las próximas elecciones.

Tabla 8. Consolidación e integración de los datos cargados, y divulgación de resultados: Resumen de hallazgos de la funcionalidad

Proceso/funcionalidad evaluado de acuerdo al plan operativo	Cumple los requisitos	Desempeño / observaciones	Recomendaciones / observación
Escrutinio especial	No	No se pudo evaluar	Disponer de la infraestructura tecnológica y de software que permita la interacción con el SIEDE.
Consolidación e Integración	Si	Las funcionalidades de consolidación / integración muestran una baja eficiencia de procesamiento, lo que puede retrasar la divulgación de resultados.	Revisar los procesos de cálculo que constituyen las funcionalidades de consolidación / integración, a fin de mejorar su desempeño. Concluir con la verificación de la integración del sistema, versus la matriz de pruebas.
Enlace de datos entre "Escrutinio Especial" y el SIEDE	No	Falta de instalación del equipamiento central en el sitio denominado INFOP.	Disponer del equipamiento central en el sitio denominado INFOP y garantizar la interacción del módulo Escrutinio Especial y SIEDE para el día de la elección.
Enlace de datos entre el SIEDE y la Divulgación de resultados en la red Internet	No	No se pudo observar su operatividad durante los simulacros por no contar hasta ese momento con la disponibilidad de dicho servicio de alojamiento en un sitio de Internet dispuesto para tal fin.	Disponer para la elección del sitio de Internet dispuesto para tal fin.

Enlace de datos entre el SIEDE y Auditoría Internacional	No	Auditoría Internacional posee alojado en un servidor dispuesto por el TSE, las imágenes transmitidas desde los ATX, faltando aún que disponga de las API[4] que le permitan interactuar con el SIEDE.	La empresa MAPA debe aportar a Auditoría Internacional las API que permiten la interacción con el SIEDE.
Pruebas de Bases de datos de acuerdo a plan operativo 8.4.b	Si	Base de datos POSTGRE no se encuentra en cluster. No se pudieron practicar las pruebas del plan de contingencia	Diseñar una estrategia de contingencia para los servicios de Bases de Datos POSTGRESQL.
Operar con canal alternativo de enlace de las empresas CLARO y TIGO. 8.3.a	Si	Las empresas CLARO y TIGO solucionaron el inconveniente técnico, que impedía el uso pleno de la redundancia de las conexiones.	
5.c	No	Hasta el desarrollo del último simulacro no se obtuvo documentación formal respecto a un plan de contingencia para la infraestructura de telecomunicaciones del SIEDE, lo que representa un indicador de calidad de un proyecto de esa envergadura.	
5.c	No	Durante los tres simulacros no estuvo funcional el sitio de contingencia alterno.	Es necesario montar el equipamiento, configurarlo y dejar operativo el sitio alterno de contingencia

Elementos clave de Funcionalidad Técnica del SIEDE: Observaciones Adicionales

Tal como estaba previsto en el plan operativo, la auditoría acompañó el desarrollo de los tres simulacros realizados por el TSE, y sobre la base de la observación de 39.15% de funcionalidad y 40.46% del volumen de las actas a ser transmitidas el día de la elección, se destaca que en los segmentos de seguridad, bases de datos, infraestructura de telecomunicaciones y hardware, los hallazgos de la auditoría arrojaron resultados favorables sujetos a mejoras previo al día de los comicios.

Con respecto al software, los procesos constitutivos del SIEDE presentaron un desempeño funcional acorde a lo previsto, debiendo hacer consideraciones respecto a lo siguiente:

[4] API: Aplication Programing Interface

- El máximo nivel tensión de trabajo o stress se produjo en el tercer simulacro, en el cual transmitieron el 91% de los Kits distribuidos para ese evento, lo que representa un 39% en relación a la cantidad total de Kits en operación para el día de los comicios.
- Tal como se mencionó anteriormente, los procesos de consolidación e integración presentaron un bajo nivel desempeño para el cálculo de acumulación de resultados y la adjudicación de cargos, situación que podría repetirse el día de la votación si se considera un mayor caudal de información.

Con relación a la infraestructura en telecomunicaciones prevista en el alcance de la auditoría, hasta el tercer simulacro, se constató que:

- El enlace de datos entre los Centros de Transmisión (ATX) y la recepción de imágenes de Actas se encuentra operativo y funcional.
- El enlace de datos entre escrutinio especial y el SIEDE se encuentra operativo, restando instalar y consolidar la infraestructura tecnológica (hardware y software) donde se llevará a cabo.
- El enlace de datos entre el SIEDE y divulgación de resultados se encuentra operativo a nivel de intranet, no así a nivel de Internet.
- El enlace de datos entre el SIEDE y la Auditoría Internacional, se encuentra operativo a nivel de enlace, restando que la empresa MAPA aporte las API correspondiente para acceder a los datos del SIEDE.

Hasta el tercer simulacro, el sitio dispuesto para las contingencias no se encontraba operativo y funcional, debido a la falta de instalación y configuración del equipamiento principal. La auditoría no pudo entonces producir hallazgos sobre este componente del SIEDE.

Consideraciones de seguridad informática

La seguridad informática se constituye como una de las áreas cruciales del sistema en estudio, manifestándose de manera transversal a todos sus aspectos funcionales. En esta sección se abordan aquellos elementos considerados críticos para el buen desempeño del SIEDE y se entregan recomendaciones encaminadas a contrarrestar las debilidades y fortalecer aun más la transparencia y confianza en el sistema durante el desarrollo de los comicios.

Análisis de vulnerabilidades

De acuerdo al análisis efectuado por esta auditoría y la información entregada por el TSE, a la fecha de concluir esta auditoría no se efectuaron análisis de vulnerabilidades en los servidores de aplicaciones, firewalls, routers, y otros elementos de infraestructura que requieren de dicha práctica. Tampoco se

realizaron pruebas respecto de las aplicaciones electorales, servidores Web y sitios Web involucrados en la divulgación de resultados.

Considerando la relevancia de la información, resulta absolutamente necesario aplicar técnicas que garanticen, más allá de la seguridad física, la integridad de los datos que se almacenan. La aplicación de barreras y procedimientos que resguardan el acceso a los datos y permiten su consulta solo a personas específicamente autorizadas resulta fundamental. A modo de prevención, se recomienda analizar la fortaleza de seguridad de forma periódica y sistemática, en especial antes de cada simulacro (hecho que no fue concretado) y el día previo al evento.

Se recomienda la inclusión del análisis de vulnerabilidades entre las actividades de seguridad en los días que restan hasta el evento electoral fomentando a partir de entonces su realización periódica, es decir, debe incluirse dentro de las políticas de seguridad informática del organismo electoral.

Toda vez que se comparta información o se permita publicar datos propios en sitios Web de otras organizaciones, es preciso solicitar como requisito previo la constancia de haber formalizado los análisis de vulnerabilidades en sus respectivos sitios Web. Así mismo, es dable determinar los requerimientos de seguridad para las tareas o servicios que sean llevados adelante por otras empresas u organizaciones y plasmarlos en un SLA (acuerdo de nivel de servicios), aún cuando se presuma se trata de una empresa con seguridad consolidada.

El responsable de seguridad para un evento electivo supervisará generalmente las tareas de análisis de vulnerabilidades y verificará la aplicación de todas las actualizaciones de seguridad[5]. Dirige asimismo los tests de penetración internos y externos que se practican previo al evento electivo sobre el centro de datos y los centros de respaldo. Es recomendable formalizar pruebas de penetración de la capa de red y pruebas de penetración de la capa de aplicación. Corresponde analizar también cada función, las habilidades requeridas, el nivel de acceso necesario, las condiciones de trabajo y el o los componentes sobre los cuales pueda impactar una vulnerabilidad detectada.

El personal del TSE debe poder llevar adelante los análisis rutinarios, a fin de mantener el nivel de seguridad logrado de manera autónoma e independiente.

Actualizaciones de seguridad en los servidores

A partir del análisis de la auditoría, se detectó que no se han efectuado los análisis de vulnerabilidades en los servidores del Centro de Procesamiento de Datos (CDP). Si bien es posible practicarlos en el tiempo que resta para el desarrollo de los comicios, su análisis en un ambiente de simulacro hubiese significado una oportunidad única para analizar su eventual comportamiento y detectar intentos de

5Es recomendado leer la guía OWASP actualizada al momento de su actuación.

penetración u otra acción maliciosa tratando de aprovechar debilidades a los sistemas de protección.

Los atacantes o hackers, mediante conductas dolosas, utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los fabricantes del producto. La Política de Seguridad del TSE precisa establecer los protocolos para instalar estos parches en los sistemas. Todos los sistemas importantes deben poseer la última versión de los parches adecuados para estar protegidos contra la explotación de los datos que, en el caso de un proceso electivo, es considerada "crítica" por el riesgo que representan a la seguridad los delincuentes y el software malicioso.

Los parches de software adecuados para instalar antes del proceso electoral son aquéllos que han sido evaluados y probados para confirmar que no crean conflicto con las configuraciones de seguridad existentes. Es por ello que se recomienda deshabilitar durante el evento electoral la funcionalidad de actualización, para evitar una descarga que provoque efectos indeseados.

En el caso de las aplicaciones desarrolladas internamente por la institución, es posible evitar numerosas vulnerabilidades mediante la utilización de procesos estándares de desarrollo de sistemas y técnicas de codificación segura (calidad en el desarrollo).

Además de la adecuada gestión de las actualizaciones de seguridad, es necesario se revise de manera periódica la configuración de seguridad de los servidores utilizando las herramientas de análisis apropiadas, adecuando los permisos, privilegios y demás aspectos según las recomendaciones del fabricante.

Cabe destacar, que pese a no existir un manual de Políticas de Seguridad Informática con sus respectivos procedimientos asociados, se constató que en el área de monitoreo de firmas, transcripción y verificación de actas y monitoreo de inconsistencias se ha actuado eficazmente, implementando medidas de seguridad en todas sus capas del modelo Open System Interconection (OSI).

Contrariamente a lo antes descrito, no se han llevado adelante las tareas de análisis y hardenización (fortalecimiento de la seguridad) en el área de servidores (CPD) ni en el área de contingencias. Se deja constancia que es posible llevar adelante estas tareas en los días que restan hasta el proceso electoral.

Administración de usuarios en los servidores

En la jornada previa al evento electoral es imprescindible deshabilitar todos los usuarios que no están autorizados a operar el día de los comicios, renovar la totalidad de las passwords y dejar un solo administrador, hasta culminar todas las tareas del evento electoral sobre los servidores, routers y elementos de seguridad.

La presente auditoría no ha podido constatar dicha buena práctica, por no contar con el acceso ni los informes de los análisis del nivel de seguridad de los servidores ubicados en el CPD ni los destinados al área de Contingencia.

Monitoreo de tráfico

El monitoreo de tráfico en un evento electoral debe abarcar tanto la red interna como los servidores Web encargados de la publicación de los resultados, sean internos o expuestos a Internet. Se trata de una combinación software - hardware que practica el monitoreo permitiendo a las administraciones actuar de inmediato ante la detección de eventos anómalos.

La auditoría pudo constatar que no se dispone a la fecha de un estándar para el monitoreo de tráfico. Se recomienda por ende el desarrollo del correspondiente estándar de configuración, definiendo las alertas predeterminadas en las que el "agente de monitoreo" debe prevenir a los administradores.

Es necesario definir claramente los pasos a seguir ante la detección de eventos anómalos o no autorizados. Este monitoreo debió ser uno de los ejes centrales de las tareas tecnológicas del personal de seguridad durante los diferentes simulacros.

Plan de respuesta a incidentes de seguridad

El plan de respuesta a incidentes es un elemento irrenunciable para el TSE. Los datos electorales son de interés público y por su naturaleza confidenciales, por lo que deben extremarse los cuidados en su administración. La experiencia comparada sugiere la implementación de un plan de respuesta a incidentes que sirva para responder de inmediato ante un evento que afecte a cualquiera de sus componentes, y fundamentalmente a los considerados estratégicos. Deben establecerse, documentar y distribuir los procedimientos de respuesta ante incidentes de seguridad informática, con la correspondiente secuencia de escalamiento para garantizar un manejo oportuno y efectivo de todas las situaciones.

Es importante que el plan cuente con una referencia o inclusión de procedimientos de registro formal y notificación inmediata a las autoridades del TSE en casos de compromiso o afectación de datos electorales. Igualmente crucial es que exista la consideración y especificación de los procedimientos para facilitar, en caso de resultar pertinente, el análisis post incidente. Esto conlleva un efectivo aporte a la transparencia electoral.

Un ítem esencial es la designación de personal especializado que se encuentre disponible permanentemente para responder a las alertas durante el evento electivo. Se recomienda proporcionar y facilitar la capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad informática.

La inclusión de alertas en los sistemas de detección y prevención de intrusiones, y de monitorización de integridad de archivos también es un factor determinante. Estos sistemas de monitorización están diseñados para concentrarse en los posibles riesgos que comprometan a los datos que, en el caso electoral, son calificados como críticos. Estas alertas resultan esenciales para tomar medidas rápidas e impedir fallos y debe incluirse la documentación de dichas alertas en los procesos de respuesta a incidentes.

Plan de contingencias y continuidad del proceso

Al plantear la incorporación de tecnología y sistemas informáticos al proceso electoral, es necesario aceptar que las contingencias forman parte inherente de los mismos. Las amenazas a la información pueden provenir de muchas fuentes, tanto de origen ambiental o natural (ej.: tormentas, inundaciones, terremotos), de origen humano (ej.: inexperiencia, sabotaje, conductas dañinas, huelga) como de origen técnico (ej.: fallas del software, hardware, suministro de energía). Durante el relevamiento no se halló evidencia suficiente de un plan de contingencias integral y debidamente documentado para el proceso electoral, contemplando todos los recursos informáticos.

Lo expuesto justifica la elaboración de planes comúnmente denominados Plan de Continuidad de Negocio (BCP / Business Continuity Planning) y el asociado plan de recuperación de desastres (DRP / Disaster Recovery Planning). Ambos se hallan descritos en la norma británica BS 25999 de la Institución Británica de Normas.

Procedimiento especial para el acceso al centro de procesamiento de datos

El acceso físico a las áreas sensibles, como la sala de servidores, el enlace de comunicaciones y el *storage* que almacena datos electorales, son factores de cuidado extremo en un evento electivo.

Se recomienda que el acceso físico a la sala de servidores sea un lugar controlado con cerradura inteligente, código y sistema automatizado de huellas digitales (captahuellas). Será obligatorio el uso de gafetes de seguridad, la filmación desde distintos ángulos del CPD, con tiempo mínimo de conservación de la grabación no inferior a 60 días, y libro de visitas informatizados con conservación no menor a 90 días. El log de la cerradura inteligente, que sea resguardado por 90 días como mínimo, debe contar con los datos completos de identificación de cada persona que ingrese al CPD, motivo del ingreso, quién lo requirió y quién autorizó su ingreso.

La guarda sugerida para cada registro de seguridad del CPD debe respetarse a menos que la ley estipule lo contrario en algún momento.

Es esencial asimismo la revisión de los datos recopilados y correlacionarlos con otros registros de entradas. En caso de incidentes de seguridad informáticos, se recurrirá a estos registros para verificar los accesos al CPD.

Estándares y gestión de la configuración

A partir del análisis realizado, hemos podido verificar que no se cuenta con un estándar para la configuración, documentación y monitoreo de los elementos especiales de seguridad, servidores, firewalls y routers.

Se recomienda desarrollar un estándar de configuración, documentación y monitoreo de elementos especiales de seguridad, servidores, firewalls y routers.

Si se define el uso y la ubicación de la tecnología y los dispositivos aprobados por el organismo, el área responsable está mejor capacitada tanto para administrar y controlar las diferencias de configuración y los controles operativos como para asegurarse de que no haya ninguna "puerta trasera" disponible. Asimismo, es vital asegurar y sincronizar los archivos de configuración de routers.

Si bien los archivos de configuración en ejecución generalmente se implementan con una configuración segura, es posible que los archivos de arranque, ejecutados por los routers solamente al reiniciarse, no utilicen la misma configuración de seguridad porque sólo se ejecutan ocasionalmente y entonces pueden generarse normas más débiles que permitan a personas malintencionadas el ingreso en la red.

Como ya se mencionó, se deja constancia que el sector área de Monitoreo de Firmas, Transcripción y Verificación de Actas y Monitoreo de Inconsistencias ha formalizado una adecuada definición de políticas de seguridad en el entorno Windows.

Revisión de los logs de auditoría

Del análisis se determina que no existe un procedimiento de revisión de logs de auditoría de los servidores, firewalls, IDS[6], IPS,[7] antivirus y dispositivos especiales de seguridad. Dicho análisis debería permitir identificar en línea los eventos o actividades en los sistemas a fin de realizar un seguimiento de los sucesos de seguridad. Tampoco se encuentran definidos mecanismos de resguardo y protección de las bitácoras de auditoría.

Por último, se recomienda promover la incorporación de una herramienta para el reclutamiento de logs y registros de auditorías de orígenes heterogéneos, concentrándolos en un solo equipo y base de datos con capacidad de respaldo unificado, generación de alertas, remisión de avisos sms o por otra vía, elaboración de análisis centralizados, estadísticas integradas y habilitación de un tablero de comandos con semáforos intuitivos. Este tipo de herramientas facilitan el control y permiten un monitoreo proactivo que, durante el proceso electoral, constituye la única forma de mantener un centro unificado de control integral.

[6] Intrusion Detection System
[7] Intrusion Prevention System

Se recomienda implementar un procedimiento de revisión y resguardo de logs de auditoría.

Fuente de tiempo

Se pudo constatar que no existe una única fuente de tiempo (forma de establecer la hora en el reloj de los ATX y otros instrumentos del sistema), sino que existen diversas fuentes y protocolos usados para establecerla, generando discordancias de sincronización y problemas de análisis en los logs.

Es necesario contar con una única fuente de tiempo uniforme y confiable utilizando el protocolo adecuado. Solo de esta manera se puede hacer un análisis integrado de logs y construir evidencia, en caso que sea necesario.

Licencias de software

Esta auditoría no contempla en su marco de actuación la constatación de licencias ni la legalidad de las mismas, pero es dable dejar expresa constancia que en caso de no contar con el debido licenciamiento, un elemento de la infraestructura (por ejemplo servidores, atc, estaciones de trabajo) puede dejar de recibir las actualizaciones de seguridad del fabricante, lo que lo expone a los riesgos de nuevas vulnerabilidades detectadas que no serían mitigadas con nuevos parches o actualizaciones de seguridad.

Conclusiones en materia de seguridad

El análisis de la seguridad de los distintos elementos del SIEDE ha demostrado que el sistema presenta, a la fecha de este informe, algunos vacíos en la implementación adecuada de medidas de seguridad que en la elaboración de este tipo de proyectos deben ser consideradas como normas mínimas que garanticen la integridad del sistema.

Tal como lo ha expresado el TSE, debido fundamentalmente a los cortos tiempos con los que se han contado para la implementación del sistema de transmisión, se han quedado fuera de la arquitectura hasta ahora elementos que colaboran a aumentar la seguridad del proceso. Cabe mencionar que de acuerdo a la experiencia comparada, los procesos acá descritos pueden ser implementados en los días que restan para el desarrollo de los comicios.

IV.- Conclusiones Generales

Por medio de la revisión de los elementos técnicos del SIEDE que estará implementando el TSE para las elecciones de Noviembre de 2013, la MOE/OEA pudo constatar que durante el desarrollo de las actividades de esta auditoría, los distintos aspectos del proyecto SIEDE, tales como: hardware, software, telecomunicaciones y seguridad, han ido evolucionando, incorporando mejoras y corrigiendo asuntos críticos para el éxito del proyecto. Por tanto, las siguientes conclusiones se refieren al desempeño del sistema hasta el día 16 de noviembre de 2013, fecha en la cual se realizó el último simulacro al sistema. De esta manera, existe la posibilidad de que las recomendaciones vertidas en el presente documento hayan podido ser implementadas con posterioridad al último simulacro y que el proyecto continúe experimentando adecuaciones y mejoras previo al día a las elecciones.

Considerando que la prueba del sistema constituye un espacio privilegiado para observar el comportamiento general de los distintos componentes que conforman el proyecto SIEDE, esta auditoría ha dado especial importancia al análisis de resultados de los tres simulacros desarrollados por el TSE. En este sentido, es importante destacar que los tres procesos ya mencionados se llevaron a cabo sin la totalidad de las funcionalidades previstas y con pruebas de carga inferiores a los objetivos definidos para esta auditoría. Por este motivo, los hallazgos se refieren fundamentalmente al comportamiento funcional durante el desarrollo de los simulacros, sin posibilidad de proyectar comportamientos con volúmenes de información y carga esperados el día de los comicios.

En cuanto a las condiciones técnicas de funcionamiento observado, las funcionalidades de escaneo, impresión y transmisión de actas desde los centros de votación, recepción de actas digitalizadas, retransmisión de actas a partidos políticos y auditoría internacional y análisis de consistencia de las actas transmitidas, transcripción y veririficacion de actas, y monitoreo de inconsistecias que integran el sistema son funcionales, cumpliendo con los parámetros establecidos dentro del proceso del SIEDE. No resultó funcional, hasta el momento de esta auditoría, la consolidación e integración de los datos cargados y divulgación de resultados. El análisis no permite, sin embargo, proyectar su desempeño con el caudal esperado para el día de los comicios. A modo de conclusión, a continuación se sintetizan los principales hallazgos relativos a la calidad y transparencia del sistema.

Calidad

En relación a la evaluación de la calidad del SIEDE, es necesario mencionar que la ausencia de manuales de requerimientos y procedimientos constituye un impedimento para el análisis del proyecto en base a métricas de cumplimiento de estándares. Del mismo modo, es necesario aclarar que los hallazgos de la auditoría han sido establecidos en base a estimaciones hechas a la fecha del cierre del presente informe, por lo que el sistema en su conjunto puede presentar mejoras en los días que restan hasta el desarrollo del proceso electoral.

Como se menciona en el cuerpo de esta auditoría, la seguridad del sistema tiene un impacto transversal a las distintas funcionalidades del SIEDE. En este sentido, retrasos en el aprovisionamiento de productos informáticos para completar la infraestructura de seguridad y una planificación tardía de estos módulos ha redundado en la existencia de vulnerabilidades que se detallan en la sección correspondiente y que requieren de inmediata atención por parte del TSE.

Relacionado con la consolidación, integración y divulgación de resultados, la auditoría pudo observar problemas en el diseño de los sistemas y algoritmos aplicados que podrían afectar su operatividad de no mediar medidas correctivas. Debido a que es un área que afecta también la transparencia del sistema, se constituye en un elemento crítico toda vez que puede afectar la calidad del SIEDE en su conjunto.

En relación a la calidad del software, la auditoría constató la corrección, fiabilidad, eficiencia, integridad y facilidad de uso, que en su conjunto constituyen elementos de buenas prácticas internacionales para el desarrollo de programas.

Los módulos que comprenden el tratamiento de actas, incluyendo el escaneo, impresión y transmisión, recepción de actas digitalizadas, retransmisión a partidos políticos y auditoría internacional, análisis de consistencia de las actas transmitidas, transcripción, verificación de actas y monitoreo de inconsistencias cumplen con los estándares de calidad requeridos para este proceso en particular. Se conservó la integridad de los datos transmitidos mientras que los resultados obtenidos y entregados a las siguientes etapas fueron correctos.

En relación al módulo de consolidación, integración y divulgación de los resultados la auditoría detectó fallas que evidenciaron el no cumplimiento con estándares de calidad requeridos para este tipo de programas. Es importante destacar que aspectos como corrección, fiabilidad y eficiencia no han sido cumplidos por estos módulos hasta la finalización de los simulacros.

En lo referente a la divulgación de los resultados, la auditoría pudo evidenciar problemas de diseño que obligaron a un rediseño de la aplicación. Por dicho motivo a la fecha no ha sido posible realizar un análisis de vulnerabilidades toda vez que no se cuenta con una versión definitiva del programa.

Transparencia

En relación a la introducción del SIEDE para estas elecciones, la MOE/OEA desea resaltar que se haya implementado una recomendación del último informe de Misión que contribuye a modernizar el proceso y agregarle aún más elementos de transparencia.

Más específicamente en relación a la transparencia que introduce el SIEDE al proceso electoral, la auditoría desea destacar que el sistema, desde un punto de vista de su funcionalidad, constituye en su conjunto un importante avance en garantizar el acceso a la información tanto a los partidos políticos, a la Auditoría Internacional y a la ciudadanía en general.

El manejo secuencial de la información, desde que el acta es escaneada y transmitida, pasando por su retransmisión a los partidos políticos hasta su divulgación definitiva en caso de consistencias en las información, permitirá a los distintos actores del proceso electoral ir conociendo los resultados bajo criterios de ordenamiento de cola sin intervención de factores adicionales, ofreciendo garantías de transparencia y equidad en la entrega de la información.

Del mismo modo, los módulos encargados de la digitación y validación de las actas mediante sistemas de revisión ciego, con verificación cruzada y capas de validación en casos de inconsistencias, cumple con garantizar un manejo de los datos de manera transparente, respetando las preferencias de la ciudadanía durante el proceso electoral.

Producto de las brechas existentes entre las pruebas de carga logradas durante los simulacros, y la información que el sistema deberá procesar el día de la elección, el área de consolidación e integración presenta una especial preocupación, toda vez que se observó un bajo desempeño en los sistemas de cálculo de acumulación de resultados y adjudicación de cargos. Esto es crucial en cuanto a la capacidad del TSE de poder generar oportunamente resultados oficiales en cuanto a las candidaturas favorecidas por el electorado. Por ello resulta prioritario optimizar los mecanismos utilizados en el procesamiento de la información y concluir con las tareas de verificación, a fin de validar que los resultados que arroja el sistema sean los correctos. En este sentido, la imposibilidad de obtener resultados en los tiempos previstos podría afectar las expectativas de transparencia esperada con la aplicación del sistema.

V.- Agradecimientos

La Misión de Observación Electoral de la OEA desea reconocer los esfuerzos de Tribunal Supremo Electoral en la implementación y puesta en marcha del sistema, y espera que las recomendaciones emanadas en este informe puedan aportar al buen desempeño del SIEDE el día de los comicios.

Finalmente, la MOE/OEA desea agradecer al TSE por la confianza depositada en la OEA para la realización de este trabajo. Del mismo modo, desea reconocer y agradecer el apoyo financiero que los Estados Miembros y Observadores Permanentes otorgan a las actividades de Observación Electoral dentro de las cuales se enmarcó este trabajo.

Anexos

I. Requerimientos de acuerdo al plan operativo.

1. Documentación general requerida:

a. Reglamento definitivo del SIEDE.

b. Ciclo de vida del proyecto SIEDE, es decir, aquella documentación técnica del proyecto que indique las etapas y procesos que se han desarrollado para el mismo.

c. Plan de Seguridad física y lógica en Telecomunicaciones.

d. Plan de Seguridad Física del Centro de Procesamiento, sitio para Contingencia y los inmuebles relacionados al Proyecto SIEDE.

e. Plan de Simulacro de cada área que involucra el SIEDE, indicando las tareas a desarrollar, actores, y si se requiere una coordinación entre las áreas involucradas y etapas, incluyendo las características del plan de contingencia de cada área.

f. Planificación del conjunto de casuística, de los datos contenidos en las Actas de Cierre, que permita accionar la totalidad de las combinaciones de posibilidades que se puedan presentar en el escrutinio, para llevar a cabo en cada simulacro nacional.

g. Plan de implementación de infraestructura tecnológica con diagramación de servidores, sus funcionalidades, e interrelaciones.

h. Documentación de Infraestructura y Telecomunicaciones enmarcadas en esta Auditoría: a saber Diagramación, Plan de Simulacro y Contingencia.

i. Documentación de la administración de las Bases de Datos enmarcadas por esta auditoría: a saber Diagrama Lógico y Físico, Plan de Simulacro y Contingencia.

j. Plan de Entrega del hardware, telecomunicaciones y esquema de seguridad del SIEDE.

2.- Documentación particular requerida para los módulos alcanzados por esta Auditoría:

a. Ciclo de vida del proyecto SIEDE, toda aquella documentación técnica del proyecto que indiquen las etapas y procesos que se han desarrollado para el mismo.

b. Cronograma de Actividades.

c. Plan de Entrega del software del SIEDE.

3.- Software:

a. Con respecto al software que se empleará en cada una de las etapas o módulos del SIEDE, enmarcada en el alcance de esta Auditoría, es necesario indicar la gestión de software, o plan técnico, que garantice de manera comprobable y verificable que se esté utilizando la última versión del software, al momento de los simulacros y el día del escrutinio.

b. Permitir la revisión conjunta con el personal técnico designado por el TSE, del código fuente de los módulos alcanzados por esta Auditoría, a fin de verificar que éste cumpla con los casos de uso estipulados (los cuales equivalen a las validaciones o requerimientos que debe cumplir el software y que han sido estipulados por el TSE) y que esta Auditoría considere críticos para el proyecto SIEDE.

c. Posibilitar la revisión conjunta del software complementario (aquel bajo la dirección, verificación, intervención y supervisión directa del TSE, por ejemplo el de divulgación) bajo el alcance de esta Auditoría, vinculados al proyecto SIEDE.

d. Revisión conjunta, con el personal técnico designado por el TSE, de la gestión del registro de eventos (logs) que posibiliten el rastreo del historial de acciones, que cada módulo o aplicación que el SIEDE tiene dispuesto. Tal como el registro de incorporación y actualización de datos, registros de fecha, hora y ubicación desde donde se efectuó cada operación; así como todos aquellos que considere el Proyecto SIEDE, enmarcado en el alcance de esta Auditoría.

e. Mecanismo de verificación de autenticidad (firma digital y encriptación) así como la integridad del archivo (cálculo de hash o equivalente) que contiene la imagen escaneada del Acta de Escrutinio de una mesa y por cada nivel electivo, que es enviada desde el Centro de Transmisión (ATX) y recibida en el Centro de Procesamiento del SIEDE.

f. Posibilitar el acceso para poder evaluar el software que interviene durante el flujo de las Actas de Cierre desde su recepción en el Centro de Procesamiento, pasando por los controles automatizados intermedios y hasta el momento de su divulgación, con la finalidad de conocer si existe algún mecanismo de ordenamiento de las Actas de Cierre, en condiciones de ser divulgadas.

g. Mecanismos de control en relación a la ejecución, configuración e

instalación de aplicaciones en los equipos utilizados en el proyecto SIEDE, dentro del alcance de esta Auditoría, con la finalidad de determinar que únicamente sea permitida la ejecución de software previamente designado. Además de imposibilitar el uso e instalación de cualquier otra aplicación.

h. Mecanismos de control de acceso de usuarios autorizados por el TSE para acceder a los equipos utilizados en el proyecto SIEDE, dentro del alcance de esta Auditoría.

i. Mecanismo empleado para retransmitir las Actas de Cierre desde el Centro de Procesamiento hacia los servidores dispuestos por el TSE, para los partidos políticos y Auditoria Internacional, previo a la validación de firmas digitales.

j. Mecanismo de licenciamiento de software instalado en el equipamiento informático dispuesto por el TSE para el SIEDE, enmarcado en esta Auditoría.

k. Posibilitar el acceso al servidor de aplicaciones dispuesto por el TSE para el SIEDE, dentro del alcance de esta Auditoría, las funcionalidades que posee, así como también el esquema de seguridad para acceder y utilizarlas, y los operadores autorizados para su administración.

4.-Hardware:

a. Con relación al Kit Tecnológico, se evaluará el mecanismo de preservación física que asegure que éste permanezca intacto en las distintas etapas por las cuales debe pasar, además se constatarán las medidas que permitan identificar las personas autorizadas para manipularlo, con la finalidad de evitar su desnaturalización (alteración) física y lógica, y si se lleva registro de quienes operan o intervienen en cada momento con el Kit Tecnológico en sus distintas etapas.

b. Posibilitar información sobre la diagramación de arquitectura de los servidores dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría, así como su distribución de planta en el Centro de Procesamiento y el sitio dispuesto para las contingencias.

c. Diagramación de arquitectura de los equipos de usuarios (estaciones de trabajo) dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría, así como su distribución de planta en el Centro de Procesamiento y el sitio dispuesto para las contingencias.

d. Acceso a información sobre el plan para el aseguramiento de la continuidad operativa, ante la falta de suministro eléctrico en: instalaciones, inmuebles y

puntos críticos del Proyecto SIEDE

e. Permitir la observación funcional del hardware durante los simulacros, de manera conjunta al personal técnico designado por el TSE, con la finalidad de analizar la presencia de potenciales inconvenientes o vulnerabilidades en relación al Kit Tecnológico, servidores, ordenadores e instrumental de telecomunicaciones o los que considere pertinentes esta Auditoría.

f. Con relación a los servidores utilizados en el proyecto SIEDE, dentro del alcance de esta Auditoría, posibilitar el acceso para revisar los logs (registros) activos que poseen configurados, observando que operadores tienen acceso a ellos.

5.-Infraestructura de Telecomunicaciones

a. Diagramación de arquitectura de telecomunicaciones (enlaces y activos) dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría, así como su distribución de planta, en el Centro de Procesamiento, el sitio dispuesto para las contingencias y los Centros de Transmisión.

b. Revisión conjunta con el personal dispuesto por el TSE, del plan de aseguramiento de las telecomunicaciones en relación a los enlaces de datos, dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría, con la finalidad de que sean exclusivos y cuenten con mecanismos de encriptación.

c. Plan de Contingencia para la infraestructura de telecomunicaciones, previsto en las distintas etapas del proyecto SIEDE, dentro del alcance de esta Auditoría.

d. Permitir el acceso para observar de manera conjunta con personal técnico designado por el TSE, la presencia de logs (registros) configurados en los equipos de redes y telecomunicaciones; con la finalidad de identificar que datos se almacenan en ellos, si el contenido se sobre escribe o almacena totalmente y nómina de operadores que poseen acceso a su configuración.

6.-Bases de Datos:

a. Diagramación de arquitectura de bases de datos que permita visualizar la función que desarrolla cada una de ellas en el proyecto SIEDE, así como su distribución de planta en el Centro Procesamiento y el sitio dispuesto para contingencias. Incluso aquellos servidores que se utilizan como repositorio de datos.

b. Diagrama de roles y funciones de los operadores de cada base de datos, dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría.

c. Revisión conjunta con el personal dispuesto por el TSE, de los mecanismos de acceso a las bases de datos, dispuestos para el Proyecto SIEDE, dentro del alcance de esta Auditoría.

d. Conocer el mecanismo, dispuesto para el Proyecto SIEDE, dentro del alcance de esta Auditoría, para la puesta en cero de los datos[8], de la totalidad de las bases vinculadas al SIEDE, y observar si contempla la posibilidad de realizar respaldos de las mismas.

e. Conocer el mecanismo, que después de haber finalizado el Primer Turno de Transcripción[9], a las 03:00 horas del 25 de noviembre de 2013, detenga el funcionamiento de las bases de datos dispuestas para el Proyecto SIEDE, con la finalidad de obtener los respaldos correspondientes.

f. Con relación a los servidores utilizados en el proyecto SIEDE, dentro del alcance de esta Auditoría, que alojan bases de datos y archivos conteniendo retransmisión de las Actas de Cierre; estos últimos dispuestos por el TSE para los partidos políticos y Auditoría Internacional; revisar en ambos casos los logs (registros) activos que poseen configurados, observando que operadores tienen acceso a ellos.

7.-Seguridad

a. Informar la diagramación de roles y funciones para la administración de seguridad, en servidores, a nivel de Sistema Operativo y Base de Datos, dispuesto para el Proyecto SIEDE, dentro del alcance de esta Auditoría, en las distintas etapas en que intervienen y conforman el proyecto.

b. Posibilitar el acceso para la revisión conjunta con el personal dispuesto por el TSE, del esquema de seguridad previsto para el acceso a los servidores donde serán replicados los archivos provenientes de los Centros de Transmisión, bajo la responsabilidad del TSE.

c. Esquema de seguridad propuesto por el TSE, para el equipamiento e infraestructura tecnológica y de telecomunicaciones, considerado crítico y de acceso restringido, de uso por el proyecto SIEDE en el alcance de esta Auditoría.

d. Posibilitar el acceso a fin de revisar de manera conjunta con el personal

[8] Reglamento SIEDE, artículo 7: Puesta en Cero de las bases de datos de resultados y de divulgación

[9] Reglamento SIEDE, artículo 24: Primer Turno de la Transcripción

dispuesto por el TSE, el plan de seguridad con cortafuegos (firewall), tanto de hardware como de software, así como los esquemas de seguridad dispuestos para las zonas protegidas y desmilitarizadas (DMZ), empleado para el proyecto SIEDE, en el alcance de esta Auditoría.

e. En función de los resultados obtenidos en el punto c., acceder a información respecto a la identificación de los puntos críticos de la infraestructura tecnológica y de telecomunicaciones, e informar el plan de detección de vulnerabilidades y las acciones contempladas para dicho plan. Todo esto con relación al proyecto SIEDE y al alcance de esta Auditoría.

f. Plan de Contingencia ante la denegación de servicio (DoS) y/o ataques informáticos en los servidores, contemplados en los Módulos previstos en el proyecto SIEDE y al alcance de esta Auditoría.

g. Esquema de seguridad a nivel de sistema operativo y de bases de datos, del mismo modo conocer el plan de actualización de parches de seguridad, en los servidores relacionados al proyecto SIEDE, y alcanzados por esta auditoría.

8.-Plan de Simulacro:

8.1.-Software:

Para cada simulacro el TSE debe disponer de los insumos y elementos tecnológicos de telecomunicaciones, hardware, software y plan de seguridad implementados.

Se requiere aplicar en cada simulacro pruebas de esfuerzo o pruebas de stress, bajo las siguientes condiciones:

a. En los tres simulacros previstos se pondrán a prueba todas las etapas del Proyecto SIEDE que estén contempladas dentro del alcance de esta Auditoría.

b. En los tres simulacros deberán funcionar y transmitir al Centro de Procesamiento, al 100% de los Centros de Transmisión (ATX) previstos para el SIEDE a fin de que los hallazgos y las recomendaciones que se produzcan se realicen con base en una verificación completa del sistema.

c. En los tres simulacros se dispondrá y se transmitirá al menos el 80% de las actas por cada nivel electivo, distribuidas en la totalidad de Centros de Transmisión; señalando que alcanzando dicha proporción de actas, generará una tensión de trabajo en los sistemas bastante próximo a una situación real (prueba de estrés). Estas deberán contemplar las diversas posibilidades que se pueden presentar durante el llenado de las Actas de Cierre.

d. En los tres simulacros se debe disponer de la totalidad del personal operativo y técnico que participará en los comicios del 24 de noviembre del año en curso.

8.2.-Hardware:

a. Quitar de manera total el suministro de energía eléctrica que alimenta el Centro de Procesamiento dispuesto para el SIEDE, para poner a prueba el funcionamiento del equipamiento de provisión de energía secundario y observar el impacto al funcionamiento integral del SIEDE.

b. Provocar un apagado abrupto del Kit Tecnológico, escogido de manera aleatoria, en circunstancia que se encuentre transmitiendo Actas de Cierre y observar el comportamiento en el SIEDE.

c. Quitar el suministro eléctrico de manera abrupta a una computadora que se encuentre en proceso de transcripción de Actas en el Centro Tecnológico, escogida de manera aleatoria, a fin de observar el comportamiento en el SIEDE.

8.3.-Infraestructura de Telecomunicaciones

a. Coordinar con las empresas Claro y Tigo, la posibilidad de desconectar durante el simulacro, la desactivación del canal de comunicación que se encuentra activo y pasar a operar con otro canal alternativo, observando el impacto en la transmisión de las Actas de Cierre desde los Centros de Transmisión.

8.4.-Bases de Datos

a. Proceder a la ejecución del mecanismo de puesta en cero de los datos en las bases de datos y servidores de archivos que almacenan las imágenes de las actas; elementos éstos dispuestos por el TSE, bajo el alcance de esta auditoría.

b. Proceder al apagado lógico de las bases de datos alojadas en los servidores que utiliza el SIEDE, dentro del alcance de la Auditoría, a fin de observar el comportamiento de dicho sistema.

8.5.-Seguridad

a. Poner a prueba la posibilidad de que usuarios no autorizados ingresen en aquellos servidores y ordenadores dispuestos por el TSE que participan en el SIEDE.

II. Hallazgos de Seguridad Informática

Hallazgo	Recomendación	Acción / Prioridad	Plazo	Inversión
El mecanismo de actualización (inventario y/o estado) de los ATX no está integrado a una Gestión Integral de Activos y Gestión de la Configuración y no posee todos los datos del activo (EQUIPO, MODEM, etc.), lo que impide una adecuada acción ante casos como el que ocurrió en que no llegaron en repliegue algunos modems y equipos componentes de ATX. Esto puede dificultar alguna reacción de emergencia durante el proceso.	Relevar todos los datos de cada activo y registrarlos con la metodología actual. Para futuros procesos, se recomienda contar con una gestión integrada de activos en la cual los ATX estén completamente identificados (con sus datos técnicos específicos) y claramente especificada su ubicación actual, así como el responsable asignado y encargado de retirarlo para el repliegue.	3	Largo	Mediana
No se cuenta con un procedimiento debidamente documentado para la instalación del software y configuración de los ATX.	Resulta elemental contar con un procedimiento que detalle las tareas para la instalación del software y parametrización de los ATX, por lo que se recomienda el desarrollo, documentación y publicación del mismo.	3	Corto	Baja
No se cuenta con un análisis de vulnerabilidades de los sitios Web ni de la aplicación Web a publicar en Intranet e Internet	Al publicar datos en la Web durante el proceso electoral, resulta imperioso formalizar previamente el análisis correspondiente a cada uno de los sitios y para ello es importante contar con personal idóneo y las herramientas apropiadas, bajo licencia o libres. Es preciso promover asimismo la capacitación del personal del TSE. Se constató la presencia de personal que asiste como parte de una cooperación horizontal con la autoridad electoral de Panamá que puede abordar estas tareas antes del evento electoral.	1	Corto	Mediana
Vulnerabilidad detectada en el sitio Web del TSE el día 14 de junio de 2013. WebDAV	Es extremadamente riesgoso exponerse a un proceso electoral con publicación Web sin antes haber resuelto los problemas de seguridad del propio sitio Web de la autoridad electoral. Evitar toda posibilidad de	1	Urgente	Baja

	durante el evento electoral.			
No se cuenta con un análisis de vulnerabilidades de los servidores de aplicaciones que se utilizarán durante el evento electoral.	El uso de servidores en un proceso electoral siempre debe ir precedida de un respectivo análisis de vulnerabilidades. Resulta además prudente extender el universo de servidores analizados a la totalidad de los existentes en el Centro de Procesamiento de Datos. Es recomendable asimismo promover en un futuro, la capacitación del personal del departamento de informática del TSE y es también vital seleccionar las herramientas apropiadas para cada modelo de servidor, sistema operativo, tipo de aplicaciones y servicios activos.	1	Corto	Baja
Ausencia tanto de un plan debidamente documentado de manejo de vulnerabilidades como de análisis y control del riesgo (comúnmente llamado gestión del riesgo).	Se debe implementar, al menos provisoriamente, una matriz de valoración del riesgo determinando su estrategia de mitigación, cálculo del riesgo residual y nivel de riesgo asumible (aceptación del riesgo). Posteriormente se recomienda formalizar un plan de manejo de vulnerabilidades y control de riesgos con el auxilio de herramientas informatizadas y alineado a alguno de los estándares reconocidos en esta materia..	2	Largo	Mediana
Los servidores instalados en el Centro de Datos no han tenido un análisis de su línea base de configuración.	Deberá analizarse su línea base y documentarse. El proceso electivo siempre debe iniciarse con las actualizaciones instaladas y probadas a fin de disponer de las soluciones a debilidades conocidas y resueltas por el propio fabricante. Como última tarea de la jornada preelectoral, debe desactivarse la instalación de actualizaciones y sólo mientras duren las tareas del acto electivo.	1	Corto	Baja
No se previeron pruebas de seguridad sobre los servidores internos de publicación antes del tercer simulacro.	Deben efectuarse pruebas previas al día de los comicios de todas las aplicaciones destinadas a publicaciones, forzando situaciones y siguiendo un estricto plan previamente definido. Se debe asimismo concretar un último análisis de vulnerabilidades y mitigar cualquier riesgo detectado. No formular dicho plan y/o no concretar las pruebas aludidas aumenta la vulnerabilidad del sistema.	1	Medio	Baja
No se previeron pruebas sobre los servidores internos de consolidación antes del tercer simulacro.	Es imprescindible elaborar un plan detallado de pruebas de los servidores afectados a la consolidación, tanto de los originales como los destinados a contingencia. Una vez aprobado, las pruebas deben implementarse de manera sistemática hasta lograr su superación de manera exitosa. No concretar las pruebas aludidas aumenta la vulnerabilidad del sistema.	1	Medio	Baja
No se dispone aún de las medidas de seguridad (documentadas) solicitadas a la	Es esencial elaborar el documento de requerimientos de seguridad y formalizar un SLA en el que queden claramente definidas las prestaciones y requisitos de performance y seguridad.	1	Corto	Baja

empresa que alojará los servidores para la publicación de resultados. No se ha elaborado un SLA (Acuerdo de Nival de Servicios) con la misma.				
No se halla instalada aún la sala de contingencia para el evento electoral.	Es imprescindible la prueba de los diferentes elementos de la infraestructura induciendo la contingencia durante los simulacros a fin de dejar debidamente probados los mismos para proceder ante una contingencia durante el proceso. Se recomienda la inmediata instalación y realización de todas las pruebas previstas antes del evento electoral.		Corto	Baja
No se efectuaron análisis de vulnerabilidades de los canales de comunicación alternativos ubicados en la Sala de Contingencias.	Se constató que no se había practicado ningún análisis pese a hallarse instalados elementos de comunicación (no así los servidores definitivos de esa sala). Se deben analizar las vulnerabilidades de todos los canales que puedan ser utilizados para la transmisión de resultados provisorios el día de los comicios.	1	Corto	Baja
No se contó con un Plan de Contingencias debidamente documentado.	Definir un Plan de Contingencias contemplando todos los elementos del sistema e infraestructura involucrados en el proceso, con sus respectivos remplazos en caso de fallas o pérdidas de performance. El Plan debe definir, entre otros extremos, los roles de cada actor, los emplazamientos y almacenamiento de componentes, rutas, tiempos, teléfonos de contacto o secuencia de autorización y activación de recursos de respaldo. No contar con el plan aludido puede generar incertidumbre en caso de existir una contingencia durante el evento electoral.	3	Medio	Media
No se dispone de un manual de Políticas de Seguridad Informática y sus respectivos procedimientos.	Es esencial contar con un manual que especifique las políticas de seguridad informática , además los procedimientos de seguridad debidamente documentados	2	Largo	Media
No se cuenta con procedimiento formal y documentado de hardenización de los equipos equipados con Windows y que forman parte del Kit Tecnológico.	Se debe contar con un procedimiento formal debidamente documentado para garantizar la adecuada configuración de los equipos.	2	Medio	Media

Ausencia de un procedimiento o política que defina la realización de un análisis de vulnerabilidades de la red.	Medio	Baja	TSE	Baja
Ausencia de un procedimiento de respuesta ante incidentes de seguridad informática.	Medio	Mediana	TSE	Mediana
Ausencia de estándares y mecanismos de control para los medios de comunicaciones (routers y firewalls).	Medio	Mediana	TSE	Mediana
No se llevó a cabo una revisión de los logs ni de los equipos de comunicación, ni de los servidores ni de los antivirus durante los simulacros.	Corto	Mediana	TSE	Mediana
Ausencia de un procedimiento especial de seguridad física en el Centro de Procesamiento de Datos (CPD). Ausencia tanto de identificación especial automatizada como de registros de visitas, autorizaciones, motivos y tareas.	Se recomienda una cerradura con control de huella dactilar y/o clave de acceso, obligatoriedad del uso de gafetes de seguridad, filmación desde distintos ángulos del CPD con tiempo mínimo de conservación de la grabación no inferior a 60 días y libro de visitas. La autorización para acceder al Centro de Procesamiento de Datos debe emanar de un único responsable. El acceso físico a los servidores es un factor de cuidado extremo en procesos electorales.	1	Corto	Mediana
Se observó y documentó fotográficamente que la puerta de acceso desde la escalera lateral hacia el CPD se hallaba abierta.	Es imprescindible que se evite el acceso libre al sitio donde se hallan los servidores, pese a hallarse ahí un efectivo de las fuerzas de seguridad, porque se constató que el mismo no tenía función de identificación de quienes se acercaban a los servidores.	1	Corto	Baja
Se observó y documentó fotográficamente que se dejó la ventana abierta de la sala en que se hallaban los servidores y se retiró todo el personal (tras probar por segunda vez la	Se debe evitar queden ventanas abiertas a fin de garantizar la integridad de los equipos dispuestos en el CPD.	1	Corto	Baja

redundancia de las comunicaciones de Claro y Tigo). Tras ello y durante minutos quedó la sala sin ocupantes y con la ventana abierta.				
Se constató la presencia de los discos de instalación de sistemas operativos Windows y Linux en la sala de producción durante el último simulacro.	No se debe permitir que en el ambiente de producción haya elementos que permitan la reinstalación de un sistema operativo.	1	Corto	Baja
Ausencia de un procedimiento documentado para la destrucción de medios de almacenamiento de información sensible.	Implementar un procedimiento que contemple la destrucción de los medios de almacenamiento de información sensible (incluyendo el papel) y, en caso de discos, por medio del borrado seguro. El procedimiento debe catalogar la información según el tiempo de conservación, sea legal o determinado por el propio organismo, y establecer la autorización expresa del responsable de informática para su destrucción. Contemplará asimismo la destrucción inmediata de todo medio cuando su conservación no sea necesaria. Debe evitarse además la amenaza del Trashing, consistente en rastrear entre las papeleras en búsqueda de contraseñas, directorios u otra información sensible.	3	Largo	Mediana

Escalas y leyendas:

Importancia:

Alta: el hallazgo presenta un riesgo potencial demasiado elevado que generaría un repudio generalizado en la confiabilidad del sistema.
Media: el hallazgo podría generar desconfianza en los resultados obtenidos por el sistema.
Baja: el hallazgo podría generar problemas en el buen funcionamiento del sistema.

Plazo:

Corto: aplicación en no más de 3 días.
Medio: aplicación en no más de 5 días.
Largo: aplicación en más de 5 días.

Inversión:

Bajo: no requiere inversión adicional, puede ser realizado por el personal del TSE
Mediana: requiere inversión en material educativo, capacitación y/o asistencia de un consultor especializado
Alto: requiere un presupuesto especial sustentado en la formulación de un proyecto en consultorías, compra de material, servicios, etc.