Auditoría de Sistemas.
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

11 de noviembre de 2019

REPORTE DE AUDITORÍA

Sistema de Voto por Boleta Única Electrónica

Massetti, Matias
Perotti, Tomas
Streitenberger, Agustín

Tabla de contenidos

1 - Introducción

1.1. Roles

Llevamos a cabo el proceso de auditoría en calidad de alumnos de la cátedra “Auditoría de Sistemas” dictada por el Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur.

1.2. Objetivo de la auditoría

La auditoría realizada tiene como objetivo verificar la integridad, seguridad, confidencialidad y confiabilidad del sistema de Boleta Única Electrónica (BUE). Por otro lado, es menester identificar sus debilidades con el objetivo de mitigar riesgos y asegurar la calidad del sistema a auditar.

1.3. Alcance

Con el objetivo de efectivizar el cumplimiento de los estándares de calidad esperados para sistemas de esta naturaleza, el equipo de auditoría relevó información sobre múltiples aspectos relacionados con el proceso de Boleta Única Electrónica. Entre ellos se destacan el software y hardware utilizado en vot.ar y la implementación técnica de la boleta. Abarcamos diversos procesos, como la cadena de distribución de software y hardware, la apertura de los comicios y la emisión del sufragio.

1.4. Objetivo perseguido

El objetivo perseguido durante esta auditoría estará enfocado en asegurar que el sistema de Boleta Única Electrónica satisfaga las condiciones óptimas de seguridad y controles requeridos en sistemas de esta naturaleza. A su vez, se tiene como finalidad mantener y/o mejorar la confiabilidad del sistema actual de voto.

1.5. Requerimientos de la auditoría

Fue brindado al equipo de auditoría el documento “Voto electrónico: Los riesgos de una ilusión” donde se exponen las principales dificultades y debilidades del sistema en sí.Además, se consultó como material adicional el trabajo *"El sistema de voto electrónico de la ciudad de Buenos Aires: Una solución en busca de problemas" de Enrique A. Chaparro* (a partir de ahora referenciado como **[EAC]**), buscando un enfoque más técnico.
Finalmente, también se consultó diversa documentación técnica con el objetivo de indagar aspectos específicos de ciertas tecnologías o procesos.
Basados en esta información el staff de auditoría expondrá su opinión técnica al respecto y realizará las recomendaciones correspondientes para mitigar riesgos y asegurar la confiabilidad del sistema.

1.6. Funciones auditadas

En base a la información recolectada por el staff, se procedió a auditar el proceso de sufragio comenzando por la instalación de los equipos, pasando por el proceso de voto hasta la transmisión de resultados del escrutinio. Durante este proceso, se recopiló información de los procesos manuales y/o automatizados llevados a cabo durante cada una de las etapas.

1.7. Tiempo invertido en las tareas

El tiempo invertido en la auditoría del sistema de Boleta Única Electrónica fue de 36 horas. Con un promedio de 12 horas de trabajo por integrante del staff.

1.8. Staff de auditoría

El staff de auditoría se conforma por tres estudiantes avanzados de la carrera de Ingeniería en Sistemas de Información, cuyos roles son los siguientes:

Massetti, Matías: Licenciado en Sistemas de Información, actualmente auditor de sistemas.

Perotti, Tomás: Ingeniero en Sistemas de Información, actualmente auditor de sistemas.

Streitenberger, Agustín: Ingeniero en Sistemas de Información, actualmente analista de controles internos y compliance.

2 - Comunicación de los resultados

En este apartado, se exponen las observaciones, consecuencias y recomendaciones sobre los hallazgos correspondientes a la documentación analizada.

Debilidad 1

Título: Limitación en la modificación de voto

Descripción del problema: Puede ocurrir que el ciudadano cometa una equivocación a la hora de emitir el voto (al ser un sistema tecnológico es más propenso a fallas). En estos casos no puede modificar su elección una vez que se imprimió la BUE.

Riesgo asociado: Si ocurre esta situación, el voto no se corresponde con la intención de voto del elector.

Valuación del riesgo: Medio

Posible solución o "forma" de mitigar el riesgo: Otorgar la posibilidad de que el elector disponga de una BUE adicional y destruir públicamente en su totalidad la BUE con el voto incorrecto. Además, agregar confirmación intuitiva al elector a la hora de emitir el voto.

Referencia: Vot.ar - ¿Cómo se usa?

Debilidad 2

Título: Falta de conocimientos técnicos de todos los actores del proceso electoral.

Descripción del problema: La mayoría de los actores no disponen de los recursos técnicos necesarios para llevar un control efectivo de las elecciones.

Riesgo asociado: Disminución de la confianza en el proceso electoral. Aumento de las probabilidades de fraude.

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Capacitar adecuadamente a todos los actores involucrados.

Debilidad 3

Título: Usabilidad del sistema.

Descripción del problema: El bajo nivel de usabilidad o accesibilidad para las personas que no cuenten con un buen nivel de alfabetización digital puede perjudicar el resultado del voto, e incluso si esto puede ser mitigado con la presencia de asistentes, el carácter secreto del voto desaparece

Riesgo asociado: Dificultad de uso que hace que los votantes puedan emitir votos que no reflejen adecuadamente sus preferencias o incluso que no puedan emitirlo.

Valuación del riesgo: Medio.

Posible solución o "forma" de mitigar el riesgo: Evaluar y testear el sistema en una muestra de personas de diferentes edades, niveles educativos, socioeconómicos y culturales.

Referencia: Voto electrónico: Una solución en busca de problemas **- Página 15**

Debilidad 4

Título: Individualización de la intención de voto.

Descripción del problema: La posibilidad de que las boletas cuenten con impresiones ocultas incluso en el troquel que se le entrega a la autoridad de mesa.

Riesgo asociado: Estas marcas pueden permitir inferir a posteriori la intención de voto de un elector.

Valuación del riesgo: Alto

Posible solución o "forma" de mitigar el riesgo: Permitir que el elector elija la boleta al azar.

Debilidad 5

Título: Controles de conteo en el resultado del escrutinio

Descripción del problema: No se han establecido procedimientos de control de conteo que validen, mediante una muestra estadísticamente significativa, los resultados del escrutinio provisorio realizado mediante medios electrónicos.

Riesgo asociado: Los resultados obtenidos en el conteo de votos no sean los correctos.

Valuación del riesgo: Medio.

Posible solución o "forma" de mitigar el riesgo: Establecer los procedimientos de control de conteo que validen los resultados provisorios del escrutinio.

Referencia: Voto electrónico: Una solución en busca de problemas **- Páginas 10 y 11**

Debilidad 6

Título: Introducción de nuevas fallas y vulnerabilidades

Descripción del problema: Cualquier aplicación informática se ve amenazada por la aparición de fallas y errores involuntarios (bugs). Estas debilidades pueden ser aprovechadas por agentes diversos de forma maliciosa y desapercibida.

Riesgo asociado: Los resultados de una elección pueden ser manipulados. Además, existe el riesgo de que resultados legítimos de una elección no sean aceptados ya que es imposible refutar de manera concluyente las acusaciones de manipulación.

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Se debe intensificar el nivel de testeo del software; es vital la implementación de ambientes apropiados para testing que permitan a los desarrolladores reproducir la ejecución del sistema en ambientes de producción.

Referencia: [EAC] Página 11

Debilidad 7

Título: Nueva categoría de voto.

Descripción del problema: La Acordada No 17 del Tribunal Superior de Justicia creó la categoría "voto no leído por motivos técnicos" inexistente en la legislación electoral.

Riesgo asociado: Se altera la definición legal de "voto en blanco".

Valuación del riesgo: Bajo.

Posible solución o "forma" de mitigar el riesgo: Se debe intensificar el nivel de testeo del software para mitigar la posible existencia de votos no leídos por motivos técnicos.

Referencia: [EAC] Página 19

Debilidad 8

Título: Nuevos actores del proceso electoral

Descripción del problema: Los técnicos tienen un rol tan importante como poco documentado o definido

Riesgo asociado: Libertad de los técnicos para realizar acciones en el proceso sin supervisión o autorización.

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Los partidos deberían contar con representantes técnicos competentes para supervisión.

Referencia: [EAC] Página 14

Debilidad 9

Título: Ejecución de software fuera de versión o no autorizado

Descripción del problema: El mecanismo utilizado para la entrega del código a los fiscales partidarios no asegura que dicha versión sea la que efectivamente luego corre en los dispositivos de votación.

Riesgo asociado: Las máquinas podrían correr software no auditado o con fines maliciosos, sin poder ser esto chequeado por ninguna autoridad.

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Podría modificarse la cadena de distribución del software, haciéndola más segura, o directamente optar por otras opciones como grabar el mismo en las memorias ROM de los dispositivos.

Referencia: [EAC] Página 18

Debilidad 10

Título: Puertos de fácil acceso.

Descripción del problema: La máquina vot.ar presenta puertos USB y un puerto de enlace de red Ethernet con conector rj-45. Además, se constata en algunos equipos la presencia de un cable etiquetado como JTAG, que va directo al mother.

Riesgo asociado: Se puede alterar el sistema mediante estos puertos.

Valuación del riesgo: Medio.

Posible solución o "forma" de mitigar el riesgo: restringir el acceso a los puertos, o directamente eliminarlos.

Referencia: [EAC] Página 27

Debilidad 11

Título: Modificación fraudulenta del RFID.

Descripción del problema: Es posible grabar el chip mediante un simple smartphone alterando el contenido de la BUE. A nivel software no se verifica si hay más de un voto para el mismo candidato por elector, y tampoco se limita un número máximo de votos por boleta.

Riesgo asociado: Se puede grabar información de forma que la BUE contenga múltiples votos a un mismo candidato y que el sistema no lo detecte.

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Implementar en el código controles sobre los totales de votos.

Referencia: [EAC] Página 18 y Manual chip ICODE SLIX IC

Debilidad 12

Título: Arquitectura básica del sistema Vot.ar

Descripción del problema: Vot.ar consta de dos maquinas: una que actúa como emisora del voto, y otra, invisible al público y a las auditorías, encargada de la impresión de la boleta.

Riesgo asociado: Al ser una caja negra, esta segunda máquina carece de controles por parte de autoridades o fiscales partidarios.

Valuación del riesgo: Medio.

Posible solución o "forma" de mitigar el riesgo: Documentar, publicar y auditar la arquitectura completa, incluyendo los dos subsistemas.

Referencia: El sistema oculto en las máquinas de Vot.Ar

Debilidad 13

Título: Presencia de almacenamiento permanente en subsistema ARM(manejo de impresora)

Descripción del problema: El subsistema basado en el procesador ARM posee una memoria flash (de almacenamiento permanente) integrada de 256 kbytes, que podría almacenar votos emitidos en esa mesa.

Riesgo asociado: La confidencialidad del voto se ve severamente comprometida

Valuación del riesgo: Alto.

Posible solución o "forma" de mitigar el riesgo: Como se mencionó en el riesgo 12, es necesario auditar todo el subsistema ARM, y seguramente también sea necesario imposibilitar la escritura en la ya mencionada memoria flash.

Referencia: El sistema oculto en las máquinas de Vot.Ar

3- Conclusión

3.1. Opinión de auditoría

Considerando el propósito, el alcance y las funciones auditadas previamente establecidas, pasamos a exponer la conclusión elaborada.
La opinión de auditoría es adversa, ya que si bien este sistema subsana varios tipos de fraude de otros métodos electorales, crea otras tantas nuevas posibles situaciones fraudulentas o de error, producidas por el escaso testing, la poca documentación y varios puntos conflictivos propios del desarrollo en sí.

Se recomienda un análisis más profundo en el código (sobre todo en el subsistema de impresión) detectando posibles falencias de seguridad y/o bugs que afecten el correcto funcionamiento. Complementariamente, sugerimos documentar y publicar todo el código utilizado, de modo de incluir en el proceso de auditoría y testing a diversos usuarios.

Además, creemos que es necesario detenerse sobre ciertas tecnologías complementarias que dan soporte al proceso electoral, como RFID, utilizada para grabar electromagnéticamente las boletas. El uso de esta tecnología puede desencadenar problemas ya que se ha probado que se puede sobreescribir o inutilizar los datos que almacena.

Por último, es importante revisar ciertos roles, especialmente los de índole técnica. Tanto los fiscales partidarios como los técnicos de la Junta Electoral deben tener un esquema de permisos y supervisiones estricto, evitando así situaciones indeseables.

3.2. Limitaciones de alcance

A pesar de que sería ideal que esté disponible públicamente, no pudimos acceder al código del sistema y su respectiva documentación. Esta es la principal limitación, ya que no se puede indagar directamente sobre el sistema en sí, sino sobre trabajos de terceros o sobre la documentación oficial, que es escasa.

Sería interesante también acceder a documentos funcionales como casos de uso.

Por último, esta carencia de información imposibilitó también utilizar herramientas de testing o técnicas para detectar nuevas vulnerabilidades.