SIE 2017 - Simposio de Informática en el Estado

Gestión de Riesgos del Voto Electrónico Basado en la Norma ISO 31000:2015

Lic. José Emanuel Sfeir, Victoria Sol Caparelli, Matías Granata, Mariano Vecco

Universidad Nacional de Avellaneda, Buenos Aires, Argentina.
josesfeir@gmail.com, victoria.caparelli@gmail.com,
matigranata@gmail.com, marianovecco@gmail.com

Resumen. El presente trabajo tiene por objetivo la realización de un análisis de riesgos sobre el proyecto de reforma electoral en el que se establece, entre otras modificaciones al sistema actual, el voto electrónico como mecanismo de ejercicio del sufragio. El Código Nacional Electoral (Ley Nº 19.945) establece que el voto debe ser universal, igual, secreto y obligatorio, características que podrían verse comprometidas sino se consideran que normas de verificación y reaseguro debe cumplir el nuevo sistema.

Keywords: voto electrónico, participación ciudadana, riesgos, transparencia, información pública

1 Introducción

1.1 Marco de Referencia y Escalas de Medición

Tomando como referencia la norma ISO 31000:2015 que establece principios y guías para el diseño, implementación y mantenimiento de la gestión de riesgos en cualquier contexto. Se evaluarán los mismos, identificando su área de impacto y su posible tratamiento, mediante de la utilización de indicadores que, con sus respectivas escalas, se presentan a continuación.

Frecuencia: indica la probabilidad de que ocurra el hecho incierto. Niveles: (1) Raro; (2) Improbable; (3) Moderado; (4) Probable; (5) Casi certeza.

Esfuerzo de remediación: destinado a medir los costos de reparación de las consecuencias del riesgo y de los riesgos residuales asociados. Categorizado en niveles alto, medio o bajo.

Severidad: magnitud de un riesgo, expresada en términos de la combinación de su esfuerzo de remediación y su frecuencia. Niveles: (1) Insignificante; (2) Menor; (3) Moderado; (4) Mayor; (5) Catastrófico.

Tipología del riesgo: es una clasificación del mismo de acuerdo a su origen. Se considerarán riesgos físicos y lógicos. Los riesgos físicos se refieren a aquellos que pudieran afectar la integridad física tanto del hardware utilizado como de las personas que lo fueran a utilizar, ya sean empleados o votantes. Por ejemplo, un corte de luz o un incendio. En cambio, los riesgos lógicos son los que, sin comprometer la integridad física del hardware o de las personas, pudieran comprometer el proceso de votación afectando la legitimidad del mismo. Por ejemplo, problemas en el software.

Contramedidas: es una medida que modifica el riesgo permitiendo reducir su impacto.

1.2 Consideraciones Iniciales: Alcances y Limitaciones del Análisis

Para realizar un análisis más específico se dividirá el relevamiento de riesgos del proceso electoral en tres etapas: emisión del voto, transmisión y, por último, procesamiento.

La etapa de emisión del voto incluye la participación del votante y la emisión de la boleta electrónica con la elección de su/sus candidatos.

La etapa de transmisión es aquella en la que la información acerca de los votos emitidos es enviada a los centros de procesamiento.

Finalmente, la etapa de procesamiento es en la cual, en los centros pertinentes, se procesa la información recibida y se realiza el conteo de los votos.

Cabe destacar que, el análisis presentado a continuación, pretende ser general. En primer lugar, debido a la incapacidad de conducir una investigación a nivel federal, que considere la disparidad entre factores como: el nivel de infraestructura existente, la brecha tecnológica, los desniveles educativos, las improntas socioculturales, la ausencia de cuadros técnicos capacitados, la diversidad geográfica, la falta de presupuestos apropiados y la existencia de órganos electorales con facultades y recursos insuficientes. En segundo lugar, debido a que se realiza a nivel teórico, ya que las experiencias de votación electrónica realizadas en el país no utilizan sistemas abiertos accesibles por los ciudadanos.

2 Determinación del Riesgo por Etapa del Proceso Identificada

2.1 Emisión del Voto

Riesgos lógicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Display incorrecto de candidatos	Decisión del voto	1	5	Medio	Contar con máquinas de respaldo
Borrado del chip	Validez del voto	2	5	Medio	Boleta legible por el votante
Alteración del chip	Legitimidad del acto electoral	3	5	Medio	Boleta legible por el votante
Captura de información del voto/votante a través de dispositivos electrónicos	Privacidad del voto	4	4	Medio	Impedir acercarse a las máquinas con dispositivos electrónicos (por ejemplo: celulares)
Desconocimiento por parte del votante acerca del uso de la nueva tecnología	Correcta emisión del voto	3/4	4	Medio	Campañas de capacitación acerca del uso de la nueva tecnología/máquina de prueba dispuesta en la entrada de cada colegio

Tabla 1. Riesgos lógicos de la emisión del voto

Riesgos físicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Cortes de luz	Ejercicio del voto	3	5	Medio	Generadores eléctricos de contingencia
Rotura de máquinas	Ejercicio del voto	3	5	Medio	Máquinas de repuesto
Inaccesibilidad para personas discapacitadas a la máquinas	Emisión el sufragio, universalidad del voto	4	5	Alto	Mesas especiales para discapacitados en planta baja
Incendio del lugar de votación	Ejercicio el voto, integridad de las máquinas	2	5	Alto	Planes de evacuación, asegurar la existencia de medidas necesarias para evitar y controlar incendios
Inundación	Ejercicio el voto, integridad de las máquinas	2	4	Alto	Planes de evacuación, definer planes logísticos de distribución de las máquinas
Chip roto/quemado	Ejercicio el voto	4	3	Bajo	Existencia de boletas de reemplazo
Maquina sin tinta de impresión	Ejercicio el voto	4	5	Bajo	Reemplazar las tintas
Alteración del hardware	Legitimidad acto electoral	2	5	Medio	Hardware abierto y auditable
Borrado de la boleta	Legitimidad acto electoral	3	4	Bajo	Utilizar impresión de larga vida útil

Table 2. Riesgos físicos de la emisión del voto

2.2 Transmisión del Voto

Riesgos lógicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Técnicas de intercepción	Legitimidad del proceso electoral	3	5	Alto	Métodos de encriptación adecuados
Espionaje	Conteo de votos	3	5	Medio	Realización de controles específicos de seguridad de redes

Tabla 3. Riesgos lógicos de la transmisión del voto

Riesgos físicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Corte de luz	Cortes en la transmisión de los datos	3	5	Alto	Generadores eléctricos
Corte de la transmisión	Conteo de votos	3	5	Medio	Contar con sistemas de respaldo

Tabla 4. Riesgos físicos de la transmisión del voto

2.3 Procesamiento del Voto

Riesgos lógicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Código oculto	Decisión del voto	5	5	Medio	Desarrollar un sistema de código abierto
Deficiencias provenientes de la transmisión	Conteo de votos	3	5	Medio	Almacenamiento de respaldo
Almacenamiento incorrecto en el servidor	Conteo de votos	3	5	Medio	Tener máquinas de respaldo

Table 5. Riesgos lógicos del procesamiento del voto

Riesgos físicos.

Descripción	Impacta en	Frecuencia	Severidad	Esfuerzo de remediación	Contramedida
Chips rotos/quemados	Conteo de votos	3	5	Alto	Utilizar el respaldo del voto impreso
Impresiones borrosas	Respaldo para el conteo de votos	3	5	Alto	Cambiar tipo de impresión
Incendio del Centro de Recepción, Totalización y Difusión	Conteo de votos, integridad del personal	2	5	Alto	Plan de evacuación, medidas contra incendio
Inundación del Centro de Recepción, Totalización y Difusión	Conteo de votos, integridad del personal	2	5	Alto	Ubicar los recursos tecnológicos necesarios para la contabilización en un piso superior a, por lo menos, el primer piso

Table 6. Riesgos físicos del procesamiento del voto

3 Conclusiones

Debido al contexto, los riesgos asociados son de impacto alto, ya que comprometen el derecho de los ciudadanos al ejercicio de la participación democrática.

El análisis realizado, deja en evidencia que el cambio de sistema no garantiza la confidencialidad del voto ni la transparencia del proceso electoral o la imposibilidad de fraude. Esto se debe a que, el desarrollo de técnicas más complejas implementadas de una manera tan abrupta, lleva necesariamente a que el sistema propuesto sea difícil de verificar.

Para garantizar la transparencia, el sistema debe ser auditado y analizado exhaustivamente en todas sus etapas por expertos de todo tipo, a fin de certificar la seguridad.

Para asegurar la confidencialidad del voto, el sistema no debe permitir la legibilidad del mismo por cualquier agente externo al proceso de votación.

Estas serán tareas que difícilmente se puedan llevar a cabo de manera eficiente, si no se cuenta con un marco normativo y con sistemas abiertos que puedan ser auditados por todos los ciudadanos.

Referencias

1. Norma ISO 31000: http://archivo2016.justicia2020.gob.ar/wp-content/uploads/2016/08/NORMA-31000-Gestion-de-Riesgo.pdf
2. Demostración de posibilidades de trackeo con dispositivos electrónicos en Cámara de diputados: https://www.youtube.com/watch?v=XA3JZ2HWQuA
3. Documento sobre la inconstitucionalidad de voto electrónico en Alemania. Fallo de la Corte Constitucional Alemana, traducida por Mariano Koesel: http://www.joseperezcorti.com.ar/Archivos/Comentarios_a_Fallos/20100709_S_2BvC3_07_BvC4_07_EVote_Alemania_Traduccion_Koessl_y_comentario_PerezCorti_JE_06_2010_Mx.pdf
4. Luces y sombras del voto electrónico, http://www.lanacion.com.ar/1942743-luces-y-sombras-del-voto-electronico
5. Razones que explican el naufragio de la propuesta oficial, http://www.lanacion.com.ar/1959832-razones-que-explican-el-naufragio-de-la-propuesta-oficial
6. http://www.telam.com.ar/tags/5553-voto-electronico/noticias
7. Media sanción para el voto electrónico impulsado por el PRO, https://www.pagina12.com.ar/diario/ultimas/20-312238-2016-10-20.html