CIBERSEGURIDAD ELECTORAL 2018

Roberto Velázquez Cabrera

Tlapitzalli
25 de diciembre de 2017

Esta nota fue solicitada por Jorge Santa Cruz, Subdirector Editorial de Voces del Periodista (VP)[1], para mi columna de Investigación Independiente de la sección de Opinión. Pude escribirla por haber ejercido funciones de Comisario “B” y Subdelegado de la anterior secretaria de la Contraloría General de la Federación (SECOGEF) y por mi experiencia en tareas de evaluación, computación y de auditoria de informática.

Es una aportación para tratar de enriquecer los análisis y discusiones que permitan mejorar los procesos electorales de 2018, que van a ser muy importantes para determinar el desarrollo futuro de la nación y de sus habitantes.

La ciberseguridad[2] es un tema importante para las elecciones de 2018, si se quiere evitar o disminuir la corrupción y los desvíos de recursos y resultados en los sistemas y procesos relacionados, para lograr una elección más limpia que, refleje mejor la voluntad de los electores nacionales. Ahora, mucha información se maneja por Internet.

Por desgracia, no se han encontrado normas detalladas abiertas o estudios a fondo que tengan esa finalidad, ni en los medios académicos y en los foros especializados realizados sobre ciberseguridad, ni en los documentos relacionados con la delincuencia y la corrupción al mayor nivel administrativo, menos, en los medios masivos de comunicación. La mayoría de las discusiones abiertas son muy generales y sin suficiente sustento legal y técnico, y muchas, hasta son sesgadas o parciales, como muchas de las observadas en las sesiones legislativas de las Cámaras y Comisiones

[1] http://www.vocesdelperiodista.com.mx/
[2] Ya se publicó un documento abierto sobre Ciberseguridad (http://tlapitzalli.com/BR/Ciberseguridad.pdf).

del Poder Legislativo, donde frecuentemente ni siquiera considera las opiniones fundadas de especialistas invitados de la sociedad. Varias iniciativas importantes, como algunas de las relacionadas con los temas comentados en este documento, se aprobaron con mucha premura, sin análisis de fondo y sin consultar al pueblo.

Algunos han advertido que hasta los *hakers* podrían intervenir en las elecciones de 2018[3]. Sobre las pasadas elecciones presidenciales de los EUA, han surgido opiniones y muchas discusiones sobre la posible influencia de *hakers*, que han sido muy comentados en los medios internacionales de comunicaciones[4 y 5], y han generado efectos y conflictos políticos al mayor nivel entre los poderes nacionales estadounidenses y con Rusia.

Si en las instituciones educativas superiores especializados en computación y redes de telecomunicaciones no se prepara suficiente personal en ciberseguridad, menos preparan a especialistas en auditorias de los sistemas usados para operar y vigilar las elecciones.

Existen varias formas que contribuyen a sesgar y alterar los resultados electorales. En la mayoría de ellos, los sistemas de ciberseguridad podrían ayudar a disminuirlos, aunque los que más fallan y cometen delitos o hacen fraudes son los humanos y varios operan fuera del ámbito gubernamental.

Unos actúan desde antes de las elecciones y han vivido de ellas, como: varios encuestadores, que nadie supervisa o audita y actúan como también lo hacen muchos publicistas, periodistas y locutores que se venden o son captados y viven como reyes. Existen sospechas de la participación hasta del crimen organizado del narcotráfico y de empresas nacionales y extranjeras muy poderosas, pero parece que nadie supervisa ni sus acciones, ingresos y transferencias monetarias en los bancos. Los presidentes electos de los últimos sexenios son ejemplos de ello, ya que ayudaron a imponerlos.

¿Cómo es posible que se gasten miles de millones de pesos para comprar a los deformadores de opinión, sin que existan sistemas que eviten las transferencias financieras en los bancos? o ¿Son de contado?

Otros actúan antes, durante y después de las elecciones. Por parte del Poder Ejecutivo, varias dependencias y entidades tienen atribuciones y funciones relacionadas con la evaluación y control, pero no se conocen sistemas que permitan conocerlas, evaluarlas y controlarlas abiertamente.

---

[3] http://expansion.mx/tecnologia/2017/11/28/elecciones-y-mundial-de-rusia-los-imanes-para-el-cibercrimen-en-2018

[4] https://www.nytimes.com/es/2017/09/19/rusia-facebook-perfiles-falsos-elecciones-eeuu/

[5] http://www.bbc.com/mundo/noticias-internacional-38350244

Una limitante fundamental se origina en que las dependencias que las evalúan no muestran una forma de hacerlo bien. La principal existente es la Secretaría de la Función Pública (SFP), pero ni siquiera han podido lograr lo que dicen sus documentos rectores. Por ejemplo, en la Introducción de su Metodología. Evaluación de la Gestión Gubernamental[6], se dice que:

Todas las acciones que realizan las instituciones públicas, tienen como objetivo el desarrollo socioeconómico del país, cuyo logro depende de la manera en cómo se realizan dichas acciones, es decir, de la "gestión pública".

La evaluación que utilizan no ha servido para lograr ese objetivo, ya que no ha sucedido. Su sistema de indicadores que utilizan, no sirve ni para evaluar la eficiencia y eficacia para lograr ese objetivo, mucho menos, para analizar, evaluar o fiscalizar a las dependencias gubernamentales que participan en las elecciones o en actos importantes de corrupción. En el famoso caso de la Casa Blanca, la SFP no encontró nada ilegal que pudiera ser penado y ya es un caso cerrado[7].

El sistema más importante de fiscalización de las elecciones es el del Instituto Nacional Electoral (INE). Fiscaliza a los partidos políticos y candidatos y tiene una contraloría interna, que supervisa principalmente los ingresos y gastos, pero no se sabe quién evalúa o audita su gestión. Sobre la evaluación del desempeño del INE, solo publican unos Indicadores de Evaluación de la Gestión[8], con datos de % en tablas para 2009-20010-2011, similares a los de la SFP. Esos indicadores no sirven para evaluar la fiscalización que realizan ni para evitar la corrupción electoral.

¿Cómo es posible que se gasten miles de millones de pesos para comprar millones de votos, sin que existan sistemas que eviten las transferencias financieras en los bancos? o ¿Son de contado?

¿Cómo es posible que nadie audite los sistemas que pueden alterar los resultados electorales?

¿Cómo pueden evaluarse y controlarse los sistemas electorales establecidos, si no existen ni cursos que preparen personal técnico en auditoria de redes y sistemas de datos electorales y no se conozcan públicamente auditorías técnicas realizadas?

¿Cómo es posible que no existan formas efectivas de evaluar, fiscalizar y controlar a los organismos gubernamentales que se relacionan con las elecciones?

---

6 https://www.gob.mx/cms/uploads/attachment/file/244678/Metodologia_para_la_Evaluacion_de_la_Gestion_Gubernamental__2017.pdf

7 http://www.elfinanciero.com.mx/nacional/la-casa-blanca-es-un-caso-cerrado-sfp.html

8 http://portalanterior.ine.mx/archivos3/portal/historico/contenido/Indicadores_de_Gestion_Transparencia/

Las facultades de control y evaluación de la gestión gubernamental son asignadas a los comisarios y delegados[9] de la SFP se ordenan en la Fracción XXI Art. el Ley de la Administración Pública Federal[10],

XXI. Designar y remover para el mejor desarrollo del sistema de control y evaluación de la gestión gubernamentales, delegados de la propia Secretaría ante las dependencias y órganos desconcentrados de la Administración Pública Federal centralizada y comisarios públicos de los órganos de vigilancia de las entidades de la Administración Pública Paraestatal y de la Procuraduría General de la República; así como normar y controlar su desempeño;

Por desgracia, los informes de sus resultados no son conocidos públicamente, ya que no se publican abiertamente. Ni siquiera podemos saber si han mejorado o no los informes que ahora hacen. Menos se sabe si sus observaciones son procedentes y se atienden. En el pasado los comisarios y delegados, no disponían ni de los recursos para tender bien sus funciones asignas más relevantes. Tampoco las Contralorías Internas institucionales podían auditar todos los gastos gubernamentales, ya que ni siquiera podían comprobar en la realidad los miles y miles de proyectos y gastos de los presupuestos.

Como los comisarios y delegados son los únicos que tienen esas atribuciones de evaluación y control gubernamental al mayor nivel, el no poder conocer sus informes significa que el IFE y ninguna otra dependencia o entidad federal que podría fiscalizar a las entidades, empresas y otras organizaciones que participan en las elecciones, no permiten ser evaluada abiertamente, como la Secretaría de Hacienda y Crédito Público (SHCP). Menos, es posible conocer y evaluar abiertamente sus sistemas operativos establecidos en medios y sistemas electrónicos que utilizan para fiscalizar a todos los que participan en las elecciones con fondos financieros.

Ya se han comentado hasta en los medios de comunicación casos de financiamiento y de usos indebidos para apoyar campañas de elecciones anteriores, pero no han sido detectadas y evitadas con los sistemas gubernamentales establecidos.

Las iniciativas legislativas promovidas sobre seguridad nacional, no incluyen normas para fiscalizar a los que cometen delitos en las elecciones, como la Ley de Seguridad Interior (LSI), publicada en un decreto del Diario Oficial de La Federación (DOF)[11].

El Instituto Federal de Comunicaciones (IFT), que regula las redes de telecomunicaciones no tiene facultades, sistemas o normas para fiscalizar las elecciones en los medios electrónicos. Si el IFT no atiende la seguridad de las elecciones en los medios de comunicaciones y en las redes de telecomunicaciones, lo tiene que hacer otra dependencia o entidad, como la Secretaria de Gobernación, con

[9] http://www.funcionpublica.gob.mx/pt/obligaciones_transparencia_art_7/sfp/_facultades/dcp.htm
[10] http://www.diputados.gob.mx/LeyesBiblio/ref/loapf.htm
[11] http://www.diariooficial.gob.mx/nota_detalle.php?codigo=5508716&fecha=21/12/2017

su Policía Federal, ya que cubren más los contenidos de los sistemas nacionales y estatales y municipales que operan.

Por ejemplo, la Secretaria de Gobernación ya emitió un Acuerdo sobre tecnologías de la información y comunicaciones (TIC) para el ámbito gubernamental:

ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias (MAAGTICS).[12]

Como no incluye en su texto a las elecciones, no se sabe quién puede vigilarlas y controlarlas bien, para evitar o disminuir la corrupción, la alteración de los resultados y los desvíos de recursos en los sistemas y procesos cibernéticos relacionados, para mejorar las elecciones de 2018.

Es interesante comentar los principales criterios establecidos para identificar, evaluar y autorizar proyectos de TIC:

Artículo 6.- Una vez elaborada la Cartera Ejecutiva de Proyectos de TIC conforme al proceso de Planeación Estratégica que se establece en el MAAGTICSI, se atenderá lo siguiente:

I. Las Instituciones presentarán a la Unidad, a través de la Herramienta de Gestión de la Política TIC, en el mes de octubre de cada año, la Cartera Ejecutiva de Proyectos de TIC del año siguiente; para conformar el PETIC deberán identificar como máximo 7 Proyectos de TIC como estratégicos, considerando como criterio preferentemente para su identificación, que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, de la EDN, del Programa y del Decreto. Los proyectos de TIC que conformen el PETIC se propondrán a la Unidad para su seguimiento.

Sería muy interesante conocer los proyectos que han aportado los “mayores beneficios a la población”, si la situación de la mayoría se ha deteriorado.

En el texto del Decreto de la LSI, tampoco se incluyen a las elecciones. ¿Qué mayor inseguridad puede existir en una nación, que no legislar bien sobre la vigilancia e inteligencia de acciones que pueden conducir a continuar con una mayor dependencia y menor soberanía y desarrollo, por acciones de corrupción, deformación y alteración de unas votaciones de los poderes Ejecutivos y Legislativos, nacionales y estatales?

La Contaduría Mayor de Hacienda de la Cámara de Diputados tiene atribuciones sobre auditoria y análisis de desviaciones presupuestales, como los del Artículo 3º del su Ley Orgánica[13] y la Ley de Fiscalización y Rendición de Cuentas de la Federación[14], pero el

[12] https://www.gob.mx/cms/uploads/attachment/file/59534/MAAGTICSI_compilado_04_02_2016.pdf
[13] http://www.dof.gob.mx/nota_detalle.php?codigo=4770470&fecha=29/12/1978
[14] http://www.diputados.gob.mx/LeyesBiblio/pdf/LFRCF.pdf

último informe es del ejercicio de 2016. El Informe del IFE[15] se incluye en el Capítulo VI de los Órganos Desconcentrados e incluye: Introducción; Información contable; Información presupuestaria; Información programática, y; Anexos. Muestra desviaciones presupuestales, entre otras, pero no se cometan o notan desviaciones ilegales en el ejercicio de los ingresos y gastos del IFE y de los candidatos y partidos políticos, como algunas graves que se han comentado hasta en los medios de comunicación. Parece que no incluyen auditorias técnicas de los sistemas que utilizan en las elecciones, como los cibernéticos, menos los que hacen de contado.

Existen otras que tienen atribuciones para fiscalizar fondos presupuestales que se utilizan para las elecciones, como la Fiscalía Especializada para la Atención de Delitos Electorales (FEPADE) y la Unidad de Inteligencia Financiera de la SHCP, Subprocuraduría Especializada en Investigación de Delincuencia Organizada de la SG y la Comisión Nacional Bancaria, pero no han sido efectivas, ni siquiera para evitar los desvíos ilegales o establecer castigos o sanciones, aunque haya denuncias derivadas de la Auditoría Superior de la Federación (ASF).

El tema de seguridad electoral cibernética, debería ser incluido en los análisis y las discusiones al mayor nivel y amplitud posible, si se quieren evitar o disminuir las fallas ocurridas y las deficiencias de evaluación y control en los sistemas y normas existentes.

Algunos especialistas han recomendado que en materia de ciberseguridad[16] es necesario crear y promover ambientes cooperativos entre los reguladores, administradores, operadores y proveedores de las TIC y que la educación es necesaria desde la edad temprana. Un problema para ello es que en las instituciones educativas técnicas de los TIC no se incluyen cursos sobre su normatividad y en las de los legisladores no se incluyen a las tecnologías.

Otro problema de mayor amplitud, es que en el llamado Modelo educativo 2017, ni en ningún otro documento rector nacional o sectorial, se incluyen a las “tecnologías mexicanas”. Esto significa que toda la tecnología de valor que se usa localmente es importada, como los miles de redes de datos o TIS existentes en nuestra nación. Eso significa, entre otras cosas, que los que las diseña y producen los sistemas equipos y programas son los que pueden conocerlos mejor y vigilar su funcionamiento en la realidad.

[15] http://www.cuentapublica.hacienda.gob.mx/en/CP/Instituto_Nacional_Electoral-2016

[16] https://www.gob.mx/cnbv/videos/foro-ciberseguridad-dialogo-de-cierre

En la educación y la investigación nacional, ocurre algo similar a lo que se ha constatado en mis estudios sobre resonadores y sonidos mexicanos[17]. Existen cientos de miles de artefactos sonoros milenarios y grabaciones etnológicas, resguardas en bodegas, museos y fonotecas, aunque muchos son extraordinarios y singulares en el mundo y la historia, pero ni siquiera se estudian con profundidad, ni se difunden con amplitud, principalmente porque en las escuelas de humanidades y cultura no les enseñan cómo analizarlas con técnicas científicas, principalmente porque los profesores no saben de eso y los tecnólogos académicos no se interesan en ayudar estudiar la cultura mexicana de valor. O sea, un hueco existente de cinco siglos, que podría empezar a llenarse algún día, cuando existan trabajos educativos conjuntos y colaborativos entre los de las disciplinas académicas requeridas para ello.

Comentarios recibidos

Ian Mursell de Mexicolore, quién desde el siglo pasado, difunde lo mexicano de valor como nadie más lo hace ni siquiera en nuestro país, en presentaciones de 2,000 escuelas elementales y museos de Inglaterra, comento:

"I read your article on Electoral Cybersecurity 2018 with interest and concern: it will be a miracle if the forthcoming elections in Mexico pass by fairly and without bias. How familiar this problem is to us in the UK too: I don't know if you read that just last week our Foreign Minister Boris Johnson argued in public with his Russian counterpart in Moscow over allegations of Russian cyber attacks in recent months on our institutions and infrastructure. Personally, I think our country should retaliate 'in kind', using the same methods. What a strange new world we live in…"

https://www.theguardian.com/politics/2017/dec/22/boris-johnson-tells-russia-we-will-retaliate-against-cyber-attacks

[17] http://tlapitzalli.com/spanish.html